حروب مواقع التواصل الاجتماعي

إيهاب خليفة




اعداد وتحويل مروة جمال


TELEGRAM
NETWORK

حروب مواقع التواصل الاجتماعي

إيهاب خليفة

حروب مواقع التواصل الاجتماعي

إيهاب خليفة

الطبعة الأولى: 2016

رقم الإيداع: 2015/22252

الترقيم الدولي: 9789773192501

الغلاف: مروة فتحي

60 شارع القصر العيني 11451 - القاهرة ت 27954529 – 27921943

فاكس 27947566

www.alarabipublishing.com.eg

بطاقة فهرسة حروب مواقع التواصل الاجتماعي / إيهاب خليفة.

- القاهرة: العربي للنشر والتوزيع 2016.

- ص؛ سم.

تدمك: 9789773192501 1

- الفيس بوك 2 - النت أ- العنوان 302,3

تمهيد

هل صحيحٌ ما يُقال عن مواقع ال"فيس بوك" و"تويتر" بأنها صنيعة أجهزة المخابرات الأمريكية والإسرائيلية حتى تتمكن هذه الأنظمة من معرفة ما تفكر به شعوب العالم وشعوب المنطقة العربية خصوصاً، وحتى تعرف توجهاتهم وأفكارهم ومطالبهم؟

هل وظفت "أجهزة الاستخبارات" مواقع التواصل الاجتماعي لإسقاط الأنظمة العربية ودعمت الشباب أثناء ثورات الربيع العربي مما جعل الحكومات والأنظمة العربية تسارع بإغلاق هذه المواقع بل والإنترنت كله عن دولهم؟

هل قامت إسرائيل بإنشاء تطبيق "Viber" الخاص بالمحادثات الصوتية عبر الهواتف الذكية بهدف التنصت على المكالمات الهاتفية عبر الإنترنت وتسجيلها ومعرفة ما يدور بها؟

أصلاً.. هل تطبيق "نظرية المؤامرة" ممكنٌ لتفسير ظاهرة مواقع التواصل الاجتماعي وتطبيقات الهواتف الذكية؟ وكذلك لتفسير ظواهر سياسية عجزت النظم والحكومات المستبدة عن مواجهتها؟ وعجزت الشعوب الجاهلة عن تفسيرها؟ أم أن عجز كليهما عن مسايرة التطورات التكنولوجية والمساهمة في خدمة الحياة البشرية - عبر تقديم اختراعات واكتشافات تفيد الإنسانية- هو ما دفعهم لتبني هذه النظرية؟

يُروى عن الفيلسوف "سقراط" أنه كان في جلسة مع عدد من طلابه يتناقشون حول قضية من القضايا، وجاء أحدهم وهو يتبختر في مشيته، يزهو بنفسه، معجبٌ بشكله، فنظر إليه "سقراط" مطوَّلاً، ثم قال جملته الشهيرة التي أصبحت مثلاً "تكلم حتى أراك"، أما أنا الآن فأضع تعديلات على هذه الجملة الشهيرة لتتلائم مع العصر الحالي، وأقول له "أعطني حسابك على الفيس بوك حتى أراك".

ذات مرة في فجر صيف 2011 كنت أتصفح موقع ال"فيس بوك" حينما فوجئت بصورة إحدى زميلاتي في المقترحات من الأصدقاء Suggested Friends، وأعلم أنها بالفعل مضافة ضمن قائمة أصدقائي، فهل قامت بحذفي؟! وعندما فتحت صفحتها لكي أفهم ماذا حدث، وجدت اسم فتاة أخرى غير زميلتي، وقد قامت بسرقة جميع صورها من على صفحتها، وقامت بكتابة محتوى إباحي على هذه الصور وعرضته على صفحتها، في انتحال واضح لشخصيتها الحقيقية، وإساءة لسمعتها، وتشويه لصورتها.

ومرةً أخرى، في بداية شتاء عام 2012، حينما كنت أبحث عن إحدى الشقق السكنية لشرائها، فما كان مني إلا أن بادرت بالبحث على موقع "جوجل" عن شقق للإيجار، وحينما وجدت الشقة المناسبة، وذهبت إلى مالكها، وهو أعز أصدقائي الآن، طلبت منه الإيميل الشخصي الخاص به بعد مطالعة الشقة، على أن أرسل له صور بعض الأوراق، وقد أخذت هذا الإيميل وذهبت مباشرة إلى موقع ال"فيس بوك"، لعلي أجد بعض المعلومات عن هذا الشخص وعن سلوكه وتصرفاته، حتى لا أقع ضحية لعملية نصب، فوجدت الكثير من خبراته سواء الوظيفية أو الأخلاقية عبر صفحته، بما شجَّعني على أخذ خطوة شراء الشقة دون تردد.

وفي إحدى المرَّات التي كنت أشارك فيها في مؤتمر علمي عن الأمن الإلكتروني ينظمه حلف الناتو كل عام في العاصمة الإستونية "تالين"، قابلت أحد المشاركين في المؤتمر، وكان ذلك في صيف 2015، وكعرف بين الباحثين أن يبادر كلٌ منّا الآخر بتعريف اسمه وإعطاء الكارت الشخصي الخاص به، والذي يحتوي على معلومات حول الاسم والوظيفة وبيانات الاتصال - بادرت بإعطاء الكارت الشخصي له، ولكن هذا المشارك اعتذر لي عن عدم وجود كارت شخصي معه، ولكن سرعان ما بادر وقال لي "ولكنّي لدي حساب على موقع فيس بوك". فهل يحل ال"فيس بوك" محل الكارت الشخصي؟

هذه هي بعض الأمثلة، وغيرها من الأمثلة الكثيرة التي تعرضت لها بصورة شخصية، أو تعرضْتَ لها حضرتك، أو على الأقل تعلم زميلاً لك قد تعرض لها، فلم يصبح السؤال: هل لديك حساب على مواقع التواصل؟ ولكن: كم حساباً لك على مواقع التواصل الاجتماعي؟ هل ال"فيس بوك" و"تويتر"، أم "إنستجرام" و"لنكد إن"، هل "واتس آب" و"فيبر"، أم "لاين" و"ويتشات Wechat"؟ فنادراً ما نجد أحداً – خاصةً من الشباب - ليس لديه حساب على مواقع التواصل الاجتماعي.

وحينما شهدت كيف يمكن أن تؤثر الهاشتاجات في مجريات الأحداث، وكيف أصبحت أداة لتشويه شخص، أو للدفاع عن شخص آخر، وحينما استغرقت في فهم ساحات التفاعل على مواقع التواصل، وجدت أنه عالم حقيقي، بإيجابياته وسلبياته، بحلوه ومرّه، فوجدت به شخصيات حقيقية للتعارف والتواصل وأخرى وهمية تديرها برامج كمبيوتر، ووجدت به سلعاً تجارية يمكن شرائها بصورة شرعية، وأخرى يتم تسويقها عبر سوق سوداء، ووجدت فيه أيضاً بائعات الهوى، وبائعي المخدرات والأسلحة، كما وجدت أيضاً مكاناً لمتابعة الأخبار، وفهم نبض الشارع الحقيقي، وأداة مجانية للتواصل الفعال بين الأفراد. فالمتناقضات كثيرة، والإيجابيات والسلبيات متنوعة.

فحاولت من خلال هذا الكتاب أن أضع بعض الأطر التحليلية دون تكلّف أو اصطناع مبالغ به، فالهدف هو فهم ماهية مواقع التواصل، وهل هي نفسها شبكات التواصل أم جزء منها؟ كيف نشأت؟ وما هي مراحل تطورها؟ وإلى أين سوف تصل؟ وكيف أصبحت مجالاً مفتوحاً للحروب؟ ومن يشارك فيها؟ وما هي أدوات القتال فيها؟ وما هي معايير الانتصار؟ وكيف يمكن لدولة أن تتعامل معها؟ هل من خلال الرقابة والمنع أم الإدارة والتقنين؟. أسئلة كثيرة حاولت قدر المستطاع في هذا الكتاب الصغير الإجابة عنها بصورة تخدم الباحثين والأكاديميين المهتمين بهذا المجال، وتخدم أيضاً الباحثين فقط عن المعرفة والاطلاع على الأمور.

مقدمة

هل لديك حساب على أحد مواقع التواصل الاجتماعي؟ إذا كانت الإجابة بنعم، فحدثني أكثر عن أفاتارك Avatar؟ نعم، أقصد أفاتارك، فلعله يكون أكثر تعبيراً عنك منك، بل يمكن القول أن أفاتارك هو صديقك اللدود، وعدوك الصدوق، فهل عندما تكتب تغريدة أو حالة على صفحتك الشخصية، تكون تعبيراً عن حالتك الحقيقية؟ أم عن تلك الحالة التي لم تعشها بعد وتتمنى أن تعيشها من خلال هذا الأفاتار؟ فتخلق عالماً مرجواً تتمنى أن توجد فيه، وحينما تعجز، يتولى أفاتارك هذه المهمة، ويقوم بالكتابة بدلاً من شخصيتك الحقيقية، ويتحدث بالنيابة عنك وعن أفكارك المرجوة.

فما حدث هو أنك خلقت شخصية رمزية أصبحت بمثابة "أفاتار" Avatar، يقوم هذا الأفاتار في الواقع الافتراضي بما تعجز أنت عن القيام به في الواقع الحقيقي، وبدأ هذا الأفاتار يُرسي دعائم فكره، ويخلق عالمه، ويضع شروط صداقاته، ومبادئ أفكاره، وقد استطاع "أفاتار" بعض الأشخاص أن ينشئ عالمه المستقل داخل مواقع التواصل الاجتماعي بعيداً عن عالمهم الحقيقي، وأن يخترع لغة خاصة به قد تكون بعيدة عن لغتهم الحقيقية، وبدأ هذا الأفاتار في تدعيم مكانته الافتراضية، وسلطته اللامحدودة في العالم الافتراضي الجديد، سواء بالعنف أو بالحب، سواء بالمغالاة أو بالتجاهل، وبدأ يتواصل مع أفاتارات أخرى، ويكوّن أفكاراً وينتمي إلى حركات، ويدخل في حروب، ويدافع عن مواقف، وينجذب إلى تيارات، قد تكون أبعد ما يكون عن واقعه الحقيقي.

وما أن ينضج هذا الأفاتار ليتوحد مع الشخصية الحقيقية أو يصبح عدواً لها، هنا تبدأ المعركة بينه وبين الشخصية الحقيقية صاحبة الحساب المُنشئ على أحد المواقع الاجتماعية، فإذا كانت الغلبة للشخصية الحقيقية، فسنجد أن رد الفعل المتكرر هو الذهاب إلى زر الضبط Setting بصفحته الشخصية على مواقع التواصل، واختيار زر Deactivate أو عدم تفعيل الصفحة، وإن كانت الغلبة للأفاتار، فسوف تنتقل المعركة من العالم الافتراضي، إلى العالم الواقعي، لتبدأ شخصية جديدة، غريبة الأطوار على الأهل والأصدقاء، شخصية صُنعت من تفاعلات تمت داخل الواقع الافتراضي، وكانت نهاية خط الإنتاج في الواقع الحقيقي، وبهذا يبدأ فتيل الحرب في الاشتعال، حرب يقوم بها أفاتار على مواقع التواصل، أو حرب تقوم بها أنت في الحقيقية، فحرب الحقيقة أنت أدرى وأعلم بها مني، فما هي حرب الأفاتار؟

هل تخيلت نفسك مرةً مشاركاً في حرب حقيقية، لكن لا توجد بها حدود جغرافية أو إقليمية، ولا يوجد عدو واضح يمكن تعريفه، ولا يوجد أرض يمكن احتلالها أو طرد محتل منها؟، فكما أن أدوات القتال فيها تخلو من الرصاص والطائرات والدبابات، فالخسائر ليست بها أشلاء أو ركام، وأيضاً الأسلحة المستخدمة ليست لديها قدرة على تدمير العدو أو إزالته.

نعم، إنه نوع جديد من الحروب، أو إن شئت فقل إنها "حروب الأفاتار"، تلك التي أفرزتها تكنولوجيات الاتصال، ووسّعت نطاقها شركات التواصل، وساهم في تعميم أدواتها المتصلون، فكانوا هم الجاني والمجني عليه، في معركة الفائز الرئيسي فيها، هو من يمتلك التكنولوجيا، وقادر

على تحديد اتجاهات النقاش، وتحليل المدركات، والتحكم في أفكار المستخدمين، وتوجيه أنشطتهم دون أن يشعروا.

نحن نتحدث عن نوع جديد من الحروب يندرج تحت نطاق حروب الجيل الرابع، التي تعتمد على استخدام كل الوسائل التكنولوجية والسياسية والاقتصادية والاجتماعية والعسكرية من قبل مجموعات غير نظامية؛ بهدف إجبار العدو على التخلّي عن سياساته وأهدافه الاستراتيجية، فالعدو غير معروف أو مرئي أو متكافئ في القوة، والتهديد الذي يمثله يصعب توقع مصدره، والإصابة به تفقد الدولة توازنها بأقل مجهود، وتمثل المعلومة عنصر الحسم في هذا الصراع.

ونركز فيها على نوع معين من الحروب هو حروب الشبكات Netwars والتي يقصد بها "محاولة تشويه أو تدمير أو تحوير ما يعرفه – أو يعتقد أنه يعرفه - مجموعة من الأفراد تجاه هذا العالم"، والتي تشمل استخدام كافة أنواع الدعاية ووسائل الإعلام بهدف تشويش الذهن، والتشكيك في الحقائق، ورفض المُسلَّمات، ونتعمق أكثر في هذا الكتاب بالتركيز على نوع معين من هذه الحروب، هو حروب الشبكات الاجتماعية والتي تشمل مواقع وتطبيقات التواصل الاجتماعي، فنحن نركز هنا على ورقة من غصن من فرع من أصل، بهدف رسم صورة شبه واضحة عن الظاهرة المرجو دراستها وفهمها، وعدم تشتيت الذهن أو إضاعة الجهد.

وإذا تحدثنا عن عناصر هذه الحرب فإننا نجد أن الجميع يشارك فيها، على عكس الحروب التقليدية والتي تكون بين جيشين نظاميين، أو حتى الحروب مع الجماعات غير النظامية، سواء كانت جماعات إرهابية أو عصابات إجرامية، فكل من يمتلك وصلة إنترنت سواء في الهاتف المحمول أو الكمبيوتر، ولديه حساب على أحد مواقع التواصل أو التطبيقات الاجتماعية، أصبح جزءً منها، سواء رغب في ذلك أو لم يرغب، سواء أدرك ذلك أو لم يدرك.

فما هي إذاً أدوات هذه الحرب؟ وما هو شكل الأسلحة المستخدمة فيها؟ ومن هم عناصرها الحقيقيون الذين يديرون هذه الحرب؟ وهل للجغرافيا دور في هذه المعركة؟ وكيف يمكن تحقيق الانتصار فيها؟ وهل يمكن قياسه؟ وهل هناك خسائر حقيقية أو مادية؟ وكيف نتجنب وقوعها؟ أو على الأقل نجنّب من لا يريد أن يشارك فيها عنائها. أسئلة كثيرة يسعى هذه الكتاب للإجابة عنها، مع بعض الحالات التطبيقية والتوضيحية.

وقد آثرت أن يكون هذا الكتاب بحجم صغير، حتى يسهل على القارئ مطالعته، وتكون المعلومات فيه محددة ومكثفة، دون تهويل أو تقليل، ويمكن أن يكون مرجعاً أوليّاً لدراسات وكتب قادمة تتناول القضية بالتفصيل بصورة أعمق وأعقد، ولكن هذه مجرد محاولة توضيحية وتمهيدية، فالظاهرة جديدة وحيّة، والكتابات فيها مازالت أوليّة، ومن ثَمّ يستهدف هذا الكتاب فقط تعريف المفاهيم، وتوضيح المعالم، وإبراز العناصر، حتى نعرف عن ماذا نتحدث وكيف يحدث.

وقد يلاحظ القارئ تركيز هذا الكتاب على الجانب السلبي من الشبكات الاجتماعية في اتهام صادق لإغفال الجانب الإيجابي فيها، ولعل تبرير ذلك بأن هدف الدراسة ليس توضيح مميزات مواقع التواصل الاجتماعي، فهي معروفة ولا يمكن إنكارها، ولكن تسعى إلى التحذير من بعض سلبياتها، ومحاولة تجنيب الأفراد تداعياتها.

ولكن، وحتى نضع الأمور في نطاقها الصحيح، يجب أن أوضح للقارئ أن حروب مواقع التواصل الاجتماعي ما هي إلا نتاج للتطور التكنولوجي الرهيب الذي أحدثه الإنترنت - البيئة الحاضنة لمواقع التواصل الاجتماعي - في كافة نواحي الحياة، سواء كانت سياسية أو اقتصادية أو عسكرية أو ثقافية واجتماعية، بصورة جعلت العصر الذي نحن فيه الآن هو عصر الإنترنت بامتياز، وهو ما يحاول الكتاب توضيحه في الفصل الأول منه. كما أتطرق فيه أيضاً إلى الدور الذي لعبه الإنترنت في تغيير طبيعة "الصراع" سواء كان بين الدول وبعضها البعض، أو بين الدول وغيرها من الفاعلين الدوليين. وأصبح الإنترنت بصفة عامة أحد مصادر تهديد أمن الدول والأشخاص على حد سواء، وما مواقع وتطبيقات التواصل الاجتماعي إلا أحد مصادر هذا التهديد الناجم عن الاستخدام المتزايد للإنترنت.

ثم يتحدث الفصل الثاني عن الشبكات الاجتماعية وتعريفها وأنواعها، ومراحل نشأتها، والفكرة الرئيسية التي تحكم عملها، فالتغريدات والتعليقات والصور والفيديوهات التي تظهر أمامك، والصداقات التي يتم اقتراحها، والإعلانات التي تراها، هي لوغاريتمات مطورة بذكاء. ثم أتطرق إلى الهاشتاج، وكيف أصبح وسيلة فعّالة، يلعب دروًا سياسياً لا يمكن إنكاره، من خلال تناول مميزاته وعيوبه وأبرز سماته. ولعله من الضروري معرفة كيفية نشأة أكبر شبكة تواصل اجتماعي معروفة حتى إعداد هذا الكتاب، ألا وهي شبكة ال"فيس بوك" العملاقة، ثم أتطرق إلى التداعيات المترتبة على تزايد استخدام الشبكات الاجتماعية.

وفي الفصل الثالث أتناول حروب مواقع التواصل الاجتماعي، من حيث التعريف، وأدوات التنفيذ، والخصائص العامة، ومن الذي يدير هذه الحروب، بالإضافة إلى نبذة عن بعض البرامج التي تُستخدم في إدارة هذه الحروب.

وأتطرق في الفصل الرابع إلى شكل حروب مواقع التواصل الاجتماعي في المنطقة العربية، وأبرز ملامحها وخصائصها، وكيف أثرت في تضليل أو تشويش الرأي العام، وكيف قامت بعض التنظيمات المتطرفة باستخدامها في أغراض مشروعة أو غير مشروعة.

ويحاول الفصل الخامس التوصل إلى إطار يمكن أن يسهم في التغلب على المشاكل والتهديدات الأمنية التي تطرحها الشبكات الاجتماعية، وذلك من خلال مطالعة بعض نماذج الخبرات الدولية، ومحاولة وضع صيغة لها تحافظ للفرد على أمنه في هذه الشبكات، وقبل ذلك على حريته وخصوصيته.

الفصل الأول: البيئة الحاضنة كيف غيّر الإنترنت شكل الحياة البشرية؟

عرفت الإنسانية في صراعها نحو البقاء بيئات طبيعية، سعت لاستكشافها واستغلالها وفرض النفوذ عليها، وهي الأرض أو الإقليم البري. ومع التوسع في الإقليم البري استطاع الإنسان أن ينطلق إلى بيئة أخرى وهي البحر أو الإقليم البحري. ومع تطور التكنولوجيا الحديثة والتطور من المشي إلى السيارات والدبابات ومن المراكب الشراعية إلى السفن البخارية ثم الغواصات النووية، أصبح للتكنولوجيا دور هام في حسم المعارك الحربية، فظهرت أهمية القوة البحرية إلى جانب القوة البرية. ومع التطور التكنولوجي أمكن القفز لبيئة طبيعية أخرى وهي الجو أو الإقليم الجوي، وبدأت تحلق فيه الطائرات وظهرت أهميتها في تدمير مواقع العدو والتمهيد للمعارك الحربية. ومع التطور التكنولوجي المذهل في عالم الطيران والصواريخ أمكن استغلال بيئة طبيعية جديدة وهي الفضاء الخارجي من خلال الأقمار الصناعية، وبرغم أن الفضاء الخارجي لم يتم استغلاله عسكرياً أو تجارياً مثلما تم استغلال البيئات الثلاثة السابقة إلا أنه يشكل محوراً هاماً في ربط هذه البيئات ببعضها البعض حيث تتزايد أهميته في عالم الاتصالات والمعلومات.

وبفضل ثورة المعلومات، ومع ظهور الإنترنت ومواقع الويب ظهرت لدينا بيئة أخرى وهي الفضاء الإلكتروني، وبرغم أنها تختلف عن البيئات الأربعة الطبيعية السابقة في كونها بيئة من صنع الإنسان Manmade، إلا أنها تتمتع بخصائص تشترك فيها مع تلك البيئات السابقة. فسهولة استخدامها ورخص تكلفتها ساعد على قيامها بأدوار مختلفة في الحياة البشرية سواء تجارية أو اقتصادية أو معلوماتية أو سياسية أو عسكرية أو أيديولوجية، هذا فضلاً على أنها لم تعُد حكراً على الدول فقط، وقد أصبح جليّاً أن من يمتلك آليات توظيف هذه البيئة الإلكترونية الجديدة يصبح الأكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

وقد استطاعت بعض الدول توظيف التكنولوجيا الحديثة في تعظيم قوتها، وظهر لدينا نوع جديد من القوة هو القوة الإلكترونية، حيث سعت الدول إلى الاستفادة من تلك القوة في تطوير استراتيجياتها العسكرية والسياسية من أجل حماية مصالحها الوطنية[1] ، فالدولة عادةً ما تترجم قدراتها على تحقيق أهدافها الخارجية من خلال استخدامها لوسائل مختلفة أهمها: الدبلوماسية، والقوة العسكرية، والدعاية، والأدوات الاقتصادية. ولكن أصبح من الأمور المستقرة في العلاقات الدولية أنّ مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة والتي تتمثل في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة ومن ثم برز دور القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات والقدرة على إنتاج التكنولوجيا المتطورة عن طريق الاختراع والإبداع، ظهر لدينا شكل جديد من أشكال القوة هو القوة الإلكترونية، وأصبح لديها تأثير على المستوى الدولي والمحلي. فمن ناحية، أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة على هذا الميدان موضع شك مقارنةً بالمجالات الأخرى للقوة، ومن ناحية أخرى، جعلت القوة الإلكترونية بعض الفاعلين الصغار في السياسة الدولية لديهم قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء الإلكتروني، وهو ما يعني تغيراً في علاقات القوى في السياسة الدولية[2].

حيث يستطيع أحد مستخدمي الفضاء الإلكتروني أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شلّ البيئة المعلوماتية والاتصالاتية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها البعض أو تضليل معلوماتها أو سرقة معلومات سرية عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسب، وبالرغم من فداحة الخسائر إلا أن الأسلحة بسيطة لا تتعدى الكيلو بايتس، تتمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني وبين العام والخاص وبين السري والمعلوم.

ماذا يقصد بالفضاء الإلكتروني؟

بفضل ثورة المعلومات، ومع ظهور الإنترنت ومواقع الويب أصبح الفضاء الإلكتروني أحد العناصر الرئيسية التي تؤثر في النظام الدولي بما يحمله من أدوات تكنولوجيا تلعب دوراً مهماً في عملية التعبئة والحشد في العالم، فضلاً عن التأثير في القيم السياسية وأشكال القوة المختلفة سواء كانت صلبة أو ناعمة.

وتتعدد تعريفات الفضاء الإلكتروني وتختلف، حيث عرّفه البروفيسور "جوزيف ناي" بأنه "نطاق تشغيلي Operational Domain مُحكم باستخدام الإلكترونيات لاستكشاف المعلومات عبر أنظمة مترابطة، وبنية تحتية لها[3] ".

وعرّف فريق جامعة الدفاع الوطني الأمريكية الفضاء الإلكتروني بأنه عبارة عن "مجال تشغيلي تجري فيه مجموعة من العمليات ذات الطابع الإلكتروني، ويتميز بأنه ذو طابع فريد ومتفرد، محكم بمجموعة من الاستخدامات التي تعتمد على الإلكترونيات والأطياف الكهرومغناطيسية وذلك لإنشاء وتخزين وإبدال وتبادل واستغلال المعلومات من خلال مجموعة من نظم المعلومات المترابطة والمتصلة عبر الإنترنت والبنى التحتية الخاصة به[4] ".

وبعيداً عن التعريفات الأكاديمية الرصينة السابقة، يمكن النظر إلى الفضاء الإلكتروني باعتباره مجالاً افتراضياً ينشأ نتيجة ارتباط أجهزة الكمبيوتر والخوادم Servers والنظم الإلكترونية بعضها ببعض عبر بنية تحتية، بهدف تنفيذ أوامر محددة يقوم بها المستخدم.

ويرتبط بالمفهوم السابق مفهوم آخر هو "الحرب الإلكترونية" والتي تعد جزءً من عمليات المعلومات التي يمكن أن يتم استخدامها في مستويات ومراحل الصراع المختلفة سواء كان ذلك على الجانب التكتيكي أو العملياتي أو الاستراتيجي، سواء أكان وقت سلم أو حرب أو أزمة. ويرتبط به أيضاً مفهوم آخر وهو "الإرهاب الإلكتروني" حيث يُعد الإرهاب الإلكتروني مثله مثل أي اعتداء من قراصنة هدفهم التخريب أو سرقة البيانات، ولكن الهدف في الأساس سياسي، ويسعى للإضرار بالأمن القومي للدولة وليس الحصول على بعض المكاسب الشخصية بصورة غير شرعية أو مجرد جذب للانتباه.

وقد كان لظهور الفضاء الإلكتروني والشبكة العنكبوتية أثر هام في الحياة البشرية، فسهولة الاستخدام ورخص التكلفة ساعدا على القيام بأدوار مختلفة في الحياة البشرية سواء تجارية أو

اقتصادية أو معلوماتية أو سياسية أو عسكرية أو أيديولوجية أو غيرها من المهام، فالذي يدير العالم الآن آحاد وأصفار غاية في الصغر، وقد أصبح جلياً أن من يمتلك آليات توظيف هذه البيئة الإلكترونية الجديدة فإنه سيصبح الأكثر قدرة على التأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

ويعتبر الفضاء الإلكتروني بيئة مصنوعة وحديثة؛ حيث يستجيب للتغيرات بصورة أسرع من البيئات الطبيعية الأخرى وذلك لاعتماده على التكنولوجيا الحديثة واستجابته السريعة للتطورات التكنولوجية، فإذا كان من الصعب السيطرة أو التحكم أو التنقل بين الإقليم البري أو البحري أو الجوي أو الفضاء الخارجي، فإنه يمكن التجول بلا حدود في الفضاء الإلكتروني بمجرد ضغطة على مفتاح التشغيل الخاص بالكمبيوتر، فهو يتميز بسهولة الاستخدام ورخص التكلفة وسهولة الحصول على المعلومات وتوافرها، فضلاً عن إمكانية التخفي وعدم الظهور بالشخصية الحقيقية الملموسة على أرض الواقع، وقد شجّع كل ذلك على تعدد الفاعلين المستخدمين للفضاء الإلكتروني، فشمل بذلك أفراداً وجماعات ودولاً ومنظمات دولية وشركات، كما تعددت استخداماته فأصبح له استخدامات تجارية ومالية واقتصادية وعسكرية واجتماعية وعلمية ومعلوماتية، فإذا كان من الصعب تحريك أسطول دولة معينة في المحيط أو الإقليم البحري للقيام بمهمة معينة، فإنه من اليسير جداً إرسال جيش جرّار من الفيروسات وبرامج الكمبيوتر التي تستطيع القيام بعمليات معلوماتية على قدر عال من الأهمية.

ويختلف الفضاء الإلكتروني عن الفضاء الخارجي في أن الفضاء الإلكتروني يعمل وفق قوانين فيزيائية مختلفة عن قوانين الفضاء الخارجي؛ فمثلاً لا تزن المعلومات شيئاً ولا تمتلك كتلة مادية وبإمكان المعلومات أن تظهر للوجود وتختفي منه ويتم تعديل وتبادل المعلومات خلال نظم مرتبطة بالبنية التحتية. ويتطلب الفضاء الإلكتروني وجود هيكل مادي من أجهزة الكمبيوتر وخطوط الاتصالات ومن ثم فإن ما يعمل داخل هذه الأجهزة يمثل نمطاً من القوة والسيطرة، وتصبح القيمة الحقيقية للفضاء الإلكتروني هي الاستفادة من كم المعلومات الموجودة بداخله والمساهمة في التحكم بها في إطار وشكل إلكتروني.

ويعد الفضاء الإلكتروني مجالاً عاماً وسوقاً مفتوحة، ويُظهر وجود شبكة من التواصل والعلاقات بين من يستخدمونه ويتفاعلون معه، وذلك مع انتقال كافة مجالات الحياة من إعلام وصحة وتعليم وحكومة ومواطنة واقتصاد وسياسة إلى الفضاء الإلكتروني فيما يشبه بالحياة الأخرى. وإلى جانب ذلك أصبح الفضاء الإلكتروني وسيطاً ووسيلةً في نفس الوقت لشنّ الهجوم وتنفيذ الأعمال العدائية بين الخصوم كغيره من المجالات كالجو أو الفضاء أو البحر، فهو بمثابة وسيط جديد للصراع، ويحوي الفضاء الإلكتروني كماً هائلاً ومتسعاً من الشبكات ونظم المعلومات والاتصالات التي تربطه مع الفضاء الخارجي والأقمار الصناعية، وعلى الرغم من درجة التشابه بينه وبين الفضاء الخارجي إلا أنه يختلف في أن الفضاء الإلكتروني تم بنائه من قبل الإنسان ولم يوجد في الطبيعة[5].

وتستخدم الدول الفضاء الإلكتروني لاعتبارات الأمن والقوة العسكرية بشكل جعل العديد من الدول تُدْخل الفضاء الإلكتروني ضمن حساباتها الاستراتيجية وأمنها القومي، إلى جانب دور

الفضاء الإلكتروني في تحقيق الرفاهية الاقتصادية والحصول على موارد الثروة والسلطة وتحقيق التفوق السياسي، وكذلك تعظيم معرفتها وسباقها العلمي والبحثي والقدرة أيضاً على تحقيق السلم والأمن والتفاهم الدولي من خلال دور الفضاء الإلكتروني كأداة اتصال ووسيلة إعلام دولية.

وتتضح العلاقة ما بين الفضاء الإلكتروني والأمن الدولي؛ حيث يوجد المحتوى المعلوماتي العسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي في الفضاء الإلكتروني، خاصة مع التوسع في تبني الحكومات الإلكترونية من جانب العديد من الدول واتساع نطاق مستخدمي وسائل الاتصال وتكنولوجيا المعلومات في العالم حيث تصبح قواعد البيانات القومية في حالة انكشاف خارجي، وهذا ما يعرضها لخطر هجمات الفضاء الإلكتروني إلى جانب الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريض أو دعم المعارضة الداخلية للنظام الحاكم.

كيف أثّر الإنترنت على تحولات القوة وأشكال الصراع؟

ولما للتكنولوجيا الحديثة من أثر على مفهوم القوة وتحولاتها؛ ظهر مفهوم القوة الإلكترونية Cyber Power حيث يعرّفها "جوزيف ناي" بأنها "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني، أي أنها القدرة على استخدام الفضاء الإلكتروني لخلق مزايا، والتأثير في الأحداث المتعلقة بالبيئات الواقعية الأخرى وذلك عبر أدوات إلكترونية[6] ". ويعرّفها "دانيال كويل Daniel T. Kuehl" بأنها "القدرة على استخدام الإنترنت لخلق مزايا، والتأثير على الأحداث في البيئات التشغيلية كافة من خلال أدوات القوة[7] ".

يرى "جوزيف ناي" أن القوة الإلكترونية مرتبطة بامتلاك المعرفة التكنولوجية، والقدرة على استخدامها. وهي تعني القدرة على استخدام الفضاء الإلكتروني في خلق مميزات والتأثير في الأحداث التي تجري عبر البيئات التشغيلية Operational Environments وعبر أشكال وأدوات القوة المختلفة سواء كانت عسكرية أو اقتصادية أو دبلوماسية أو معلوماتية[8] ، وقد حدد "ناي" ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية يتمثل النوع الأول في الدولة والنوع الثاني في الفاعلين من غير الدول والنوع الثالث هم الأفراد، وقد حدد "جوزيف ناي" أنماطاً لاستخدام موارد القوة الافتراضية وميّز بين الاستخدام الناعم لها والاستخدام الصلب.

ويجادل "جوزيف ناي" بأن مفهوم القوة الإلكترونية يشير إلى "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل [9]".

وتتعدد أدوات ممارسة القوة في العلاقات الدولية وفقاً لقدرات وإمكانيات ورغبات القوى المشاركة فيها، فقد تكون القوة العسكرية هي أحد أهم هذه الأدوات، وقد تكون القوة الاقتصادية والحصار الاقتصادي والمالي هو العامل الرئيسي للسيطرة على الخصم وممارسة

القوة عليه، وقد تكون الأداة المعلوماتية من خلال وسائل الاتصال والتكنولوجيا الحديثة والإنترنت هي العامل الرئيسي لحسم صراع بين دولتين.

إلا أن ممارسة القوة والنفوذ قد تطورت بشكل هائل نتيجة للتطور الكبير في المعلومات مما جعل هذه المعلومات هي الهدف الأساسي الذي تسعى الدول للحصول عليه، هذه المعلومة هي التي مكّنت الدول من إنتاج السلاح النووي، وظل هذا التطور مستمراً، حيث اعتمدت كل مرحلة من مراحل التطور الإنساني على سلطة أو قوة من طبيعة معينة تتناسب مع متطلبات هذه المرحلة.

ولقد أثرت هذه السلطة أو القوة بصورة مباشرة أو غير مباشرة في أدوات الصراع بين المجتمعات وآلياتها، وأفرزت مفردات ومكونات تكاملت معاً لتنتج نظاماً دولياً سيطرت مفاهيمه بعض الوقت أو كل الوقت، وفي هذا الإطار تميّز عصرنا الحالي بظاهرة الثورة العلمية والتكنولوجية، ولقد أزاحت وحيّدت التكنولوجيا الكثير من عناصر القوة عن مواقعها التي تربعت عليها فترة طويلة. مما عرّض المفهوم التقليدي للقوة إلى انتقادات، وأفصح عن محتوى جديد للقوة، فلم يعد ما في يد الدولة من قدرات عسكرية أو ما تمتلكه من أموال وثروات كافياً لبلورة دورها كقوة مؤثرة وفاعلة [10].

وأصبحت القوة الإلكترونية حقيقة أساسية في العالم بكل مظاهرها المتنوعة، بما عمل على دعم ومساندة العمليات الحربية والقوة الاقتصادية والسياسية، وكذلك دعم دور ثورة المعلومات والمعرفة في بروز مجتمع المعلومات الدولي والاقتصاد الإلكتروني الجديد، الذي أثر على طبيعة النظام الدولي فيما يتعلق بالتقسيم الدولي للعمل الذي يحدد آفاق النمو أمام مختلف البلاد، ويعمل أيضاً على توزيع الموارد الاقتصادية ومستويات النمو الاقتصادي، وأنماط التفاعل بين القوى الاقتصادية الدولية، والتأثير على القوة السياسية بالتأثير على عمليات صنع القرار في النظام الدولي.

ويتضمن مفهوم القوة الإلكترونية تغطية كافة القضايا التي تتعلق بالتفاعلات الدولية والتي تشمل القضايا العسكرية والاقتصادية والسياسية والثقافية والإعلامية وغيرها، وتختلف عن مسمى الحرب الإلكترونية التي تقتصر على التطبيقات العسكرية للفضاء الإلكتروني ويتم الإشارة إليه بالهجوم الإلكتروني، وقد كان لذلك أثر كبير على تغير طبيعة الصراع سواء كان بين الدول وبعضها البعض، أو بين الدول وغيرها من الفواعل الأخرى، وظهر نوع جديد من الصراع هو الصراع الإلكتروني.

تصاعد الاهتمام الدولي بالفضاء الإلكتروني خاصةً بعد ما أتاحه من أدوات وآليات جديدة عملت كوسيلة ووسيط لتهديد عمل المرافق الحيوية والبنية التحتية الكونية للمعلومات وعدم توقفها أمام سيادة الدول، بما جعلها بيئة خصبة للاستخدام غير السلمي من جانب كافة الفاعليين على تنوعاتهم المختلفة والذين تراوحوا ما بين استخدام الدول إلى الفاعليين من غير الدول، وظهر ذلك في استخدام الفضاء الإلكتروني كساحة للحرب الباردة والحرب النفسية وحرب الأفكار أو من خلال استخدامه لشنّ الحروب والإرهاب بين الدول، أو استخدام الأفراد أو الجماعات الإرهابية أو القراصنة على نحو يؤثر في الطبيعة المدنية أو السلمية للفضاء الإلكتروني.

بل إن مسار هذا التغير الذي أحدثته التكنولوجيا في حالة حركة، وهو في طريقه إلى التصاعد وطور التكوين ومن غير الممكن فهم العلاقات الدولية وظاهرة الصراع الدولي بمعزل عن التطور الذي يشكل ملمحاً لم يكتمل بعد؛ حيث يصعب تحديد آثاره وتداعياته بشكل شامل ونهائي حالياً ومستقبلاً[11] ، ومع اتساع نطاق استخدام الفضاء الإلكتروني زادت الرغبة في السيطرة عليه باعتباره ميداناً جديداً للعلاقات والتفاعلات بين الدول وبين الفاعلين من غير الدول، وأصبح سلاحاً ذا حدين، فقد يتطور الخلاف السياسي بين دولتين إلى مواجهة عبر الفضاء الإلكتروني وقد يتطور إلى إحداث أضرار مادية ضخمة وهو ما يمثل مكمن الخطورة الأكبر في درجة التأثير على الصراع الدولي، خاصة في الوقت الذي تسعى فيه جميع الدول إلى الحصول على المعلومة واقتحام أنظمة المعلومات السرية للأجهزة العسكرية والمعلوماتية.

إلا أنه يلعب في نفس الوقت دوراً في المساعدة على منع الصراعات؛ وذلك من خلال المساعدة في تقريب وجهات النظر وتبادل الأفكار والرؤى والآراء، حيث يشهد الفضاء الإلكتروني عبر الشبكات الاجتماعية والتجمعات الإلكترونية زيادة في العلاقات بين المواطنين عبر الدول، وسهولة في تبادل المعلومات والبيانات، والمساعدة في تجاوز الهياكل البيروقراطية للحكم، كما عزّز الفضاء الإلكتروني من التغيير الهيكلي للدبلوماسية بالانتقال الجزئي من الاعتماد على الدولة الرسمية إلى تفاعل جهات وجماعات وأفراد داخل الدولة، والانتقال من مرحلة تبني النموذج المركزي في صنع السياسة الخارجية إلى الانفتاح على طرق تنفيذ أهدافها، وتم تنشيط الاتصالات الداخلية ووزارة الخارجية والانفتاح على المعلومات.

ويأخذ الصراع الإلكتروني طابعاً تنافسياً حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، إلى أن يمتد ذلك الصراع إلى محاولة السيطرة على الإنترنت من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع والتحكم بالمعلومات والعمل على اختراق الأمن القومي للدول بدون استخدام طائرات أو متفجرات أو حتى انتهاك للحدود السيادية، كهجمات قرصنة الكمبيوتر وتدمير المواقع والتجسس بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر[12].

وللصراع الإلكتروني خصائص تميزه هي:

- الفاعلون الدوليّون متنوعون وفي بعض الأحيان مجهولون.

- غير مكلف مادياً أو مالياً.

- سهولة الابتداء والانتهاء.

- به جزء مادي متمثل في خضوع الأجهزة والخوادم Servers والحاسبات لسلطان الدولة وسيادتها.

- قابلية تغيير خصائصها مستقبلاً؛ نتيجة التغيرات السريعة في التكنولوجيا.

- الغالبية العظمى لا تستطيع نزع سلاح الطرف الآخر أو تدميره كلياً أو احتلال إقليمه.

- إمكانية استخدام الفضاء الإلكتروني في القوة الناعمة أو الصلبة.

كيف يصبح الإنترنت مصدر تهديد للأمن القومي؟

تتعدد مصادر تهديد الأمن القومي للدول من خلال الإنترنت، حيث تعتمد كثير من الدول في الوقت الحالي على الإنترنت لإدارة كافة شئون مواطنيها، فتبنّى بعضها نماذج الحكومة الإلكترونية، والبعض الآخر تبنى نموذج الحكومة الذكية، فأصبحت البنى التحتية تعتمد بصورة أساسية على الإنترنت، وأصبح يتم تقديم الخدمات عبر الإنترنت، وأصبحت نظم الطيران والملاحة والاتصالات والمواصلات تعتمد على الإنترنت.

ومع تزايد الاعتماد على الإنترنت في كافة مجالات الحياة سواء كانت سياسية أو اقتصادية أو عسكرية أو غيرها، ومع تحول بعض مواقع التواصل الاجتماعي لتكون فاعلاً غير تقليدي في العلاقات الدولية، أصبح الإنترنت سلاحاً ذا حدين، فكما أنه وسيلة لتحقيق الرخاء والتقدم البشري، هناك جانب آخر مظلم، يتمثل في تزايد التهديدات والمخاطر الناجمة عن الاعتماد المتزايد عليه في ظل عالم مفتوح يحكمه تفاعلات غير مرئية وغياب سلطة قانونية عليا تسيطر عليه.

وكان نتيجة لذلك أن تحول الفرد إلى فاعل دولي قائم بحد ذاته، قادر على التأثير في الأحداث الدولية، مثل نموذجي "سنودن"[13] و"أسانج"[14] ، بل أصبح الفرد قادراً على شنّ هجوم بمفرده على دولة ما، وإلحاق أضرار بها، دون أن يغادر غرفته الشخصية، وذلك من خلال هجمات إلكترونية يقوم بها ضد أهداف حيوية، مثل قواعد بيانات قومية أو عسكرية أو خدمات مالية ومصرفية أو محطات طاقة ووقود وغيرها.

ومن ثم، فقد ساهم الإنترنت في تسهيل عملية التواصل بين الأفراد وزيادة معدل الاستثمارات والتدفقات المالية، وساهم في تحقيق الرفاهية للأفراد، وساعد الدول على تقديم خدماتها الذكية بصورة توفر الوقت والجهد وتحقق الكفاءة والفاعلية، إلا أنها من جانب آخر كانت لها تأثيرات سلبية وخطيرة على الأمن القومي للدول منها:

- استهداف البنية التحتية للدولة من خلال هجمات إلكترونية تستهدف محطات الطاقة والوقود والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات.

- سرقة المعلومات والبيانات العسكرية أو التلاعب بها من خلال اختراق قواعد البيانات العسكرية أو القومية وسرقتها أو تزييفها أو تدميرها إلكترونياً.

- السيطرة على الأنظمة العسكرية، ويقصد بها السيطرة على نظم القيادة والسيطرة عن بعد بما يخرج الأسلحة والوحدات والكتائب العسكرية عن القيادة المركزية.

- الحرب النفسية الإلكترونية من خلال إرسال رسائل إلكترونية، سواء عبر البريد الإلكتروني أو الموبيل تحتوي على رسائل ترهيب أو بها مطالب محددة أو غيرها.

- الإرهاب الإلكتروني من خلال قيام بعض الأفراد المتطرفين والمتشددين دينياً بتنفيذ هجمات إلكترونية ضد أهداف افتراضية تابعة للدولة سواء كانت مواقع إلكترونية أو غيرها.

- "إثارة" أو "إعادة توجيه" الرأي العام، وهو الدور الذي لعبته مواقع التواصل الاجتماعي أثناء ثورات الربيع العربي من خلال استخدامها في عملية التعبئة العامة للجمهور وتوجيه الرأي العام بما يخدم أجندات سياسية.

- تشويه الرموز السياسية من خلال استخدام بعض الأدوات التي تتيحها مواقع التواصل الاجتماعي مثل الهاشتاج، واستخدامه في تشويه بعض الرموز السياسية أو الإساءة إليها.

- نشر الفكر المتطرف وتجنيد الأفراد، وهو أحد الإشكاليات الرئيسية التي طرحها الاستخدام المتزايد للإنترنت من خلال ربط الجماعات المتطرفة بعضها ببعض، فضلاً عن تجنيد مزيد من الأفراد من خلال الإنترنت وجمع التمويل اللازم للقيام بعمليات إرهابية.

- جمع معلومات اقتصادية استخباراتية من خلال اختراق قواعد البيانات المالية والمصرفية وقواعد بيانات الشركات والبنوك وجمع المعلومات التي قد تؤثر على الأمن القومي للدولة.

- التجسس على المسئولين والمؤسسات المالية؛ حيث نشر موقع "رويترز" خبراً يؤكد قيام الرئيس الأمريكي "باراك أوباما" بإصدار أوامر بوقف التنصت على مقري صندوق النقد الدولي والبنك الدولي وذلك في إطار مراجعة لأنشطة جمع المعلومات الاستخباراتية.

- التحويل غير الشرعي للأموال من خلال تصيد بعض عملاء البنوك عبر الإيميل ومطالبتهم بتحديث بياناتهم ومن ثم سرقتها وتحويل أموالهم لحسابات أخرى غير شرعية.

- ازدهار التجارة غير الشرعية مثل تجارة المخدرات والرقيق الأبيض والأسلحة والكتب الممنوعة وغيرها من أنواع التجارة غير الشرعية والتي تجد في الإنترنت مكاناً للازدهار.

- الابتزاز والتحرش الإلكتروني من خلال التجسس على البيانات الشخصية ومطالبة الضحية بإرسال مبالغ مالية لعدم نشر بياناتهم الشخصية.

- التأثير على الثقافات والقوميات بسبب سهولة التواصل بين مختلف الثقافات الذي قد يؤثر بدوره على هوية الأفراد، الذين قد يجدون في بعض الثقافات نموذجاً جاذباً عن ثقافتهم المحلية.

ومن ثم يتضح لنا أن ثورة المعلومات وظهور الإنترنت أثّرا على كافة مناحي الحياة سواء كانت سياسية أو اقتصادية أو عسكرية أو اجتماعية، ومع استمرار عملية تطوير الإنترنت ظهرت المدونات والمنتديات ومواقع التواصل الاجتماعي التي كان لها دور رئيسي في تغيير ثقافة الأفراد، وأصبحت أكبر تجمع افتراضي للسكان في العالم، بما تحتويه من عدد مشتركين يفوق 2 مليار مستخدم حول العالم، أي ما يقرب من ثلث الكرة الأرضية، ومع وجود هذا التجمع السكاني الافتراضي العملاق على الشبكات الاجتماعية، كان من الطبيعي أن تنتقل ساحات الصراع إليها، وباعتبارها جزءاً أصيلاً لا يتجزأ من الإنترنت، فقد أصبحت ساحة للمعارك والحروب الافتراضية، وهو ما ستتضح معالمه خلال الفصول القادمة.

كم مرةً تفتح صفحة ال" فيس بوك" أو "تويتر" الخاصة بك يومياً؟ مرة أم مرتين؟ أم أنها مرة واثنين في الساعة؟ أم أنها مرة واثنين في نصف الساعة؟ أم أنها أكثر من ذلك؟ كم عدد المشتركين في قائمة صداقاتك؟ وكم عدد الذين رفضت أن تقبلهم بسبب أسمائهم والتي كانت من قبيل "القلب المجروح – والحب الأبدي – وصغيرة على الحب" وغيرها من هذه الألقاب، كم من صديق قمت بعمل بلوك block له بسبب خلاف في الرأي أو في الموقف السياسي؟ وكم من أصدقائك وضعك في قائمة المحظورين؟

كم خبراً سياسياً أو اقتصادياً قمت بتشييره Share على صفحتك، وبعد أيام أو حتى ساعات أدركت أنه إشاعة، أو غير حقيقي، ولم تقم بتصحيح المعلومة، كما قمت بنشرها؟ كم من طفل شاركت صورته لأنه فُقد من أهله ووُجد بجوار محطة السكة الحديد؟ هل وقعت أمامك صورة تخبرك بأنك إذا لم تنشرها فإن "الشيطان قد منعك"؟ هل فكرت أكثر من مرة تفكيراً جديّاً أن تغلق صفحة ال"فيس بوك" خاصتك، وأن تبتعد عن هذا العالم، ولكن ما تلبث أن تعود إليه من جديد، فلا تستطيع نفسك أن تبتعد عنه، لأنه أصبح جزءً أساسياً منها؟

وليس من قبيل المبالغة القول أن مواقع التواصل الاجتماعي أصابت معظم مريديها بمرض الشيزوفرينيا، فهم على ال"فيس بوك" أو "تويتر" شخصية، وفي الواقع شخصية تماماً مختلفة، فغالباً ما يميلون إلى المبالغة في كل شيء، سواء في المصطلحات أو في المشاعر أو في الأفكار، فنجدهم يميلون إلى الحدة اللفظية والعبارات القاسية والألفاظ الخارجة والمنافية للآداب العامة والتي لا يستطيعون الجهر بها في التجمعات، سواء على مستوى العائلة أو العمل أو الأصدقاء، أو يمليون إلى العاطفة والرومانسية وعبارات الحب والهيام، والتي هي غالباً ما تكون أيضاً بعيدة عن سلوكهم في الواقع، أو يميلون إلى الكلام المتفلسف المعقد المعاني والمتداخل الأفكار والمتجاوز للواقع والأقرب إلى التنظير منه إلى تحديد المواقف.

إنَّ تأثير مواقع التواصل بما تلعبه من أدوار سياسية أو اجتماعية أو أمنية، هو الذي يمنعك من أن تبتعد عن هذا العالم السحري، فهو يتميز بسرعة في نقل المعلومات بين عدد كبير من المستخدمين في الوقت الحقيقي لها وبمجرد حدوثها. كما أنها لا تعترف بمناصب أو درجات أو مسميات وظيفية؛ فالجميع له نفس خصائص الصفحات، ونفس آليات التواصل، في تحقيقٍ لمبدأ التواصل بين الجميع. كما أنها لا تَعْتبر بحدود جغرافية أو سياسية.

ولعل أحد أهم مميزاتها، هي القدرة على التخفي وعدم الظهور بالشخصية الحقيقية، وهو ما يعتبر من وجهة النظر الأمنية أحد سلبياتها، ليس ذلك فحسب؛ بل أيضاً عدم القدرة على التأكد من صحة المعلومات المتداولة من خلالها أو وقف انتشارها، الأمر الذي جعل منها سلاحاً إعلامياً فعالاً، بما تمتلكه من عدد مستخدمين يقترب من 2 مليار مستخدم؛ فأصبحت أحد الأدوات الرئيسية التي يتم توظيفها في المعارك السياسية والعسكرية، لتحقيق الأهداف الاستراتيجية سواء لدولة أو جماعة ما.

وقد تميزت هذه المواقع بوجود رأي عام إلكتروني قوي يتشكل بداخلها، قادر على الانتقال السريع إلى الشارع، وأصبحت المعلومات المتوافرة عليها مادة ثرية لوسائل الإعلام التقليدية كالصحافة والتليفزيون؛ فاتجهت لنقل أخبارها وتقديم نشرات يومية عما يُثار بداخلها، وأبرزت الاتجاهات السائدة فيها، وبذلك ساهمت في وصولها لفئة جديدة، غير راغبة أو غير قادرة على الانخراط فيها، كما أنها مثّلت مصدراً هاماً للمعلومات، سواء للأفراد أو الشركات أو الحركات السياسية.

هذا الأمر هو الذي دفع بعض الدول لإنشاء كتائب وجيوش إلكترونية، مهمتها الدفاع عن صورة الدولة، والمساهمة في تحقيق أهدافها، فتشكلت جبهة حرب حقيقية موازية، ساحة القتال فيها هي مواقع التواصل الاجتماعي، وأدوات القتال هي الفكرة والمعلومة والصورة والفيديو وبرامج الكمبيوتر العملاقة، والخسائر فيها تمثل خَصْمَاً من اتجاه الرأي العام المؤيد لأحد طرفي الصراع، أو فشل الدولة في تحقيق التعبئة العامة نحو أحد أهدافها، أو انتهاك لخصوصية الأفراد وسرقة المعلومات؛ فبدا في الأفق ظاهرة جديدة قيد التشكيل، يمكن تسميتها حروب مواقع التواصل الاجتماعي.

وبصفة عامة يمكن القول، أن مواقع التواصل الاجتماعي أعادت تشكيل العديد من المفاهيم والأفكار والصناعات، فظهرت مصطلحات جديدة تتلائم مع الشبكات الاجتماعية، فكلمة Share لا تقتصر فقط على مشاركة الصور والحالات عبر ال"فيس بوك"، ولكن ظهرت في إعلانات تليفزيونية تحت شعار "شير في الخير". كما أنك إذا قولت لصديقك "ابعتلي واتس" فإنها لا تحتاج إلى إعادة تعريف، حيث يقصد بها إرسال رسالة عبر تطبيقppA s'What. وكذلك ساهمت في إنعاش سوق البرمجيات؛ فظهرت العديد من التطبيقات، سواء على مواقع التواصل الاجتماعي أو تطبيقات موبيل، تستهدف تحقيق متعة المستخدمين، وتقديم أفضل خدمة تواصل وتسلية في نفس الوقت؛ فظهر العديد من تطبيقات الألعاب على موقع ال"فيس بوك"، وتطبيقات استطلاعات الرأي، وتطبيقات التسويق، التي تستهدف تحقيق رفاهية المستخدمين. وظهر العديد من تطبيقات الموبيل سواء للدردشة النصية أو الصوتية أو عبر الفيديو، بالاعتماد على رقم الهاتف المحمول؛ فساهمت في إنعاش صناعة البرمجيات.

كما أنَّ هذه المواقع رسّخت من مفاهيم الممارسة السياسية، وأصبحت أحد أدوات صناعة الإعلام، وليست مصدراً للمعلومات فحسب، حيث اتجهت العديد من وسائل الإعلام التقليدية لهذه الشبكات لعرض ما بها من أخبار وتفاعلات وتصريحات وبيانات. وأيضاً أصبحت هذه التطبيقات بمثابة نافذة "رسمية" للعديد من الرموز السياسية للإدلاء بتصريحاتهم من خلالها، وعملت وسائل الإعلام التقليدية على خلق نوافذ صحفية لها على هذه الشبكات لعرض المحتوى الإعلامي الخاص بها عليها، حتى لا تفقد حصتها من القراءة، خاصة لدى فئة الشباب.

وقد اعتبر البعض أن مواقع التواصل الاجتماعي والشبكات الاجتماعية، ما هي إلا وسيلة للتعبير عن آراء فئة محدودة من الشباب المثقفين، الذين لديهم مهارات في استخدام الكمبيوتر والإنترنت وينتمون لطبقة اجتماعية متوسطة على الأقل؛ ومن ثم لا يشكلون رأياً عاماً حقيقياً يعبر عن مشاكل الشارع الذي تصل الأمية فيه إلى أكثر من ربع عدد السكان.

بينما نظر إليها البعض الآخر على أنها أداة رئيسية في عملية التغيير السياسي التي مرت بها بعض الدول العربية، في وقتٍ كان الإعلام الرسمي والخاص يحتفظان فيه بخطوط حمراء لا يمكن الاقتراب منها. ومثّلت أداة مهمة للنشطاء السياسيين لتحقيق عملية التواصل الفعال بينهم، وسرعة نقل أخبارهم وأماكن التجمعات وتداول خرائط التظاهرات ومعرفة أماكن تجمعات الشرطة لمحاولة تفاديها، فضلاً عن تحولها إلى منصة لنشر الانتهاكات التي تقوم بها أجهزة الأمن ضد أي من النشطاء.

كما صاحب تزايد استخدام هذه المواقع والتطبيقات الاجتماعية، تبلور عدد من الظواهر السلبية؛ مثل عمليات الابتزاز والنصب الإلكتروني، ونشر الشائعات والمحتويات غير الأخلاقية وغيرها من الجرائم الإلكترونية. إلا أن الغلبة كانت للظواهر السياسية؛ حيث تم استخدام هذه الشبكات وبخاصة ال"فيس بوك" كوسيط لعمليات الحشد والتعبئة العامة وتنظيم المظاهرات الافتراضية والاحتجاجات الفئوية، ولم يقتصر الأمر على ذلك فقط، بل شمل تحريف الحقائق وتزويرها، وتلفيق التهم، والتشهير والإساءة للسمعة، والسخرية اللاذعة، والقذف والسب. كما أصبحت الوسيلة التي تقوم من خلالها بعض الحركات الإرهابية مثل تنظيم "داعش" بتجنيد أفرادها، ونشر معلومات حول طريقة تصنيع المتفجرات والعبوات البدائية، وتنبيه بعض الإرهابيين إلى أماكن حيوية تتسبب في شلّ البنية التحتية للدولة مثل أبراج الكهرباء، وهو ما يعتبر تهديداً صريحاً للأمن القومي.

وفي ذلك ظهر نوع جديد من الحروب يمكن أن يطلق عليها حروب مواقع التواصل الاجتماعي، لها نمط معين وخصائص معينة، تختلف عن الحروب التقليدية في الأدوات، لكنها لا تقل ضرراً في التأثير؛ حيث تستهدف بنية الدولة الاجتماعية، وزعزعة استقرار النظام السياسي، وتكليف الخصم تكلفة مرتفعة لرد هذا الهجوم.

وعلى الرغم من الاعتقاد السائد بأن نشأة شبكات التواصل كانت في الأساس اجتماعية، فإن هذا الاعتقاد غير صحيح؛ فنشأة شبكة الإنترنت كلها كانت أمنية سياسية، وقد استقت أفكارها بل ومصطلحاتها من الحركات الأدبية التي كانت تدعو للثورات والتمرد على النظم السياسية، وتعتبر حركة Cyberpunk أو "الصعلوك الإلكتروني" واحدة من أقدم الحركات الأدبية التي ظهرت في ثمانينيات القرن الماضي، وتميزت بمدرسة ربطت في كتاباتها بين الواقع والتكنولوجيا والخيال العلمي، بهدف الخروج على نمطية الحياة. ودعت في كتاباتها إلى التمرد على المجتمع من خلال ثورة ثقافية، وقامت في رواياتها بتمجيد الأبطال الفرديين المتمردين على النظم الفاسدة، وأدخلت العديد من المفاهيم الجديدة مثل القرصنة الإلكترونية، وصارت هذه الحركة منبعاً فكرياً لمريدي الشبكات الاجتماعية منذ نشأتها. ومن هنا فليس هناك داعٍ للتعجب من اللغة الثورية الداعية للتمرد عبر هذه الشبكات، فهذا هو الخطاب الذي استخدمه منظّروها قبل أن توجد وذلك من خلال الروايات الأدبية والأفلام السينمائية.

أولاً: لماذا تنشأ شبكات التواصل الاجتماعي؟

يمكن إرجاع عمر شبكات التواصل الاجتماعي إلى عمر الويب Web نفسه، فمنذ اختراع صفحات الويب الخاصة بشبكة المعلومات، بدأت الأفكار تتجه نحو ربط الأفراد من خلال تجمعات

افتراضية إلكترونية، بدأت بمواقع ضعيفة وتجارب أولية لم يكتب لها النجاح. وقد يرجع ذلك إلى ضعف إمكانيات شبكة الويب حينها، وعدم تمتعها بميزات تفاعلية مثل الشات – الدردشة الفورية - أو المحادثات الصوتية أو الفيديو. وقد شهدت هذه المرحلة نشأة المنتديات التي حظيت بشعبيات عالية، ومجموعات البريد الإلكتروني مثل ال"ياهو"، ثم المدونات الشخصية، وتطورت حتى وصلت لمرحلة ال"فيس بوك" و"تويتر" و"يوتيوب" و"واتس آب".

ولم تتوقف الشبكات الاجتماعية عن التطور؛ فشهدت ظهور شبكات متخصصة مثل "لينكد إن Linked In" موقع التوظيف الأول في العالم، وغيره من المواقع المتخصصة، مثل "Academia" و"Researchgate" الذي يهتم به الباحثون والأكاديميون، وكذلك موقع "Hirepurpose" الذي يمثل تجمعاً للقادة العسكريين المتقاعدين، وموقع "Healthtap" وموقع "Sermo" الخاص بالأطباء. وإذا كانت جميع هذه المواقع السابقة تتشابه في كونها تعتمد على البيانات الحقيقية للمستخدمين، إلا أن هناك اتجاهاً آخر بدأ في الظهور، وهو الشبكات مجهولة الهوية، والتي تقوم فكرة نشأتها والاشتراك فيها على إخفاء شخصية المستخدم. وقد يرجع سبب ظهور هذه الشبكات وتطورها للتالي:

- أسباب أيديولوجية: تعكس في جوهرها الفكر الليبرالي؛ الذي يرمي إلى حرية الرأي والتعبير والانفتاح على الثقافات المختلفة في ظل عولمة الأفكار والثقافات؛ فنجد أن الحكومات التي تقوم بإغلاق مواقع التواصل الاجتماعي مثل الصين وإيران وتركيا يواجها الرأي العام الدولي الرسمي وغير الرسمي باستهجان تام، ويطالب برفع القبضة الأمنية عن الشبكات الاجتماعية، وإتاحة الحرية للأفراد للتواصل عبر هذه الشبكات؛ تدعيماً لمبدأ الحرية الفردية وحرية الرأي.

- أسباب براجماتية: تتمثل في الرغبة في تكوين صداقات والحفاظ على الصداقات القديمة بالتغلب على عوائق المكان، فكان السبب الرئيسي لنشأة شبكة ال"فيس بوك" هو تخوف مؤسسها "Mark Zuckerberg" من أن يفقد أصدقائه بعد الانتهاء من الدراسة الجامعية. بالإضافة إلى أن الشبكات الاجتماعية تمثل متنفساً للأفراد بعيداً عن الواقع التقليدي إلى واقع آخر افتراضي، يجد فيه الفرد مزيداً من الحرية. فضلاً عما تقدمه من خدمات خاصة بإنشاء الصفحات الشخصية والتجارية ومشاركة الملفات وتنظيم الفاعليات وإدارة المجموعات وتسويق المنتجات.

وقد ساهم التوجه التجاري لهذه الشبكات في زيادة نشاطها وتطوير خدماتها، فأصبحت بمثابة أسواق افتراضية لمشتركيها، ومع تطوير خصائصها امتلكت قواعد بيانات عملاقة يمكن للأفراد والشركات والدول الاستفادة منها. كما أنها وفرت عدداً من الوظائف الخاصة بالتسويق الإلكتروني وإدارة الصفحات والمجموعات، وساهمت في تنشيط سوق التطبيقات "Applications" الموجودة على مواقع التواصل.

وقد انعكس التقدم التكنولوجي في البنية التحتية والبرامجية الخاصة بالإنترنت وكذلك تطور صفحات الويب Web على تطور خصائص ومكونات الشبكات الاجتماعية، حتى أصبحنا على مشارف جيل جديد منها، ستكون اليد العليا فيه للدولة، وليس لصالح الأفراد كما هو معتقد.

ثانياً: أنواع الشبكات الاجتماعية بصفة عامة يمكن التمييز بين نوعين من الشبكات الاجتماعية؛ هي مواقع التواصل الاجتماعي مثل موقع ال"فيس بوك" و"تويتر" و"جوجل بلس" و"يوتيوب" و"إنستجرام". والتطبيقات الاجتماعية الخاصة بالهواتف الذكية، سواء كانت تطبيقات مواقع تواصل أو تطبيقات مستقلة بذاتها تعتمد على أرقام التليفون مثل "فايبر" و"لاين" و"وي تشات" و"أي إم أو IMO[15] " وغيرها من مئات التطبيقات. وفيما يلي تعريف كل منها:

1- مواقع التواصل الاجتماعي أولاً، يمكن تعريف مواقع التواصل الاجتماعي بأنها "مواقع تتشكل من خلال الإنترنت، تسمح للأفراد بتقديم لمحة عن حياتهم العامة، وإتاحة الفرصة للاتصال بقائمة المسجلين، والتعبير عن وجهة نظر الأفراد أو المجموعات من خلال عملية الاتصال، وتختلف طبيعة التواصل من موقع لآخر"[16] ، ولعل من أبرز هذه المواقع؛ ال"فيس بوك" و"تويتر" و"جوجل بلس"، و"لينكد إن"، وغيرها من المواقع المتخصصة مثل "يوتيوب" و"إنستجرام".

ولعله من اللافت للانتباه أن هذه المواقع أصبحت فاعلاً غير تقليدي في العلاقات، سواء بين الدول وبعضها البعض، أو داخل النظام السياسي نفسه؛ بين الحاكم والمحكومين. وأصبحت مواقع التواصل الاجتماعي أحد الأدوات الرئيسية، ليس فقط لمشاركة الأحداث الاجتماعية، والخواطر الشخصية، والأفكار الفردية، في إطار جمعي بين المستخدمين، أو للتعبير عن الأفكار السياسية والتوجهات الأيديولوجية والمواقف الرسمية للمسئولين. ولكن وصلت إلى مستوى أبعد من ذلك؛ فأصبحت أحد أدوات صناعة الأحداث والأخبار. وبالرغم من تعدد مميزاتها، إلا أنها تم استخدامها على مستويات تهدد الأمن القومي للدول؛ مثل تنظيم مظاهرات أو توجيه رأي عام أو جمع معلومات عامة أو تشبيك تنظيمات إرهابية أو تجارة في السوق السوداء أو جمع تبرعات لنشاطات مشبوهة أو تنظيم احتجاجات إلكترونية.

وقد برزت ظاهرة مواقع التواصل الاجتماعي بوضوح خلال ثورات الربيع العربي، وتسببت في إقلاق العديد من النظم السياسية والحكومات. واتجهت بعض الدول إلى غلقها والبعض الآخر إلى مراقبتها، خاصةً بعد أن وجدت بعض التنظيمات الإرهابية مدخلاً لتجنيد أفراد أو جمع تبرعات لها من خلالها. واستخدمتها الحركات الإرهابية والسياسية بل والدول في معاركهم الفكرية، بصورة أصبحت أقرب إلى حرب حقيقية تجري على مواقع التواصل الاجتماعي، وهو ما أبرز أهمية التعامل الجدّي مع هذه الظاهرة الجديدة.

2- تطبيقات الموبيل للتواصل الاجتماعي Mobile Apps تعد تطبيقات الهاتف المحمول هي نقطة التحول الرئيسية في الشبكات الاجتماعية؛ وهي عبارة عن "برامج يتم تحميلها بصورة مجانية أو مدفوعة عبر منصات تحميل التطبيقات مثل "جوجل بلاي" أو "أبل ستور" أو "أمازون" أو "مايكروسوفت فون". وتعتمد في عملية التواصل فيما بينها على رقم الهاتف المحمول الخاص بالمستخدم والمتصل بالإنترنت. وتستطيع هذه البرامج أن تصل إلى بيانات المستخدم على الهاتف، سواء كانت صوراً أو رسائل أو بيانات اتصالات، وأن تتعرف على أماكن تواجده، وأن تحتفظ بسجلات الدردشة الخاصة به"، ومن أمثلة هذه التطبيقات الواتس أب، وفايبر، ولاين، وبلاك بيري ماسنجر، وتوك راي، وليبون، وتليجرام، واي أم أو، وغيرها من البرامج.

ويعد التطبيق الأكثر انتشاراً في العالم، هو تطبيق What's app ؛ حيث احتل المرتبة الأولى في متجر "جوجل" و"أبل" و"ميكروسوفت" في عدة دول. يليه تطبيقات Viber وLine وTango وimoوBBM وWeChat بالإضافة إلى عدد كبير آخر من التطبيقات لكنها لا تحتل درجة متقدمة في الترتيب.

ثالثاً: كيف تعمل مواقع التواصل الاجتماعي؟

التغريدات والتعليقات والصور والفيديوهات التي تظهر أمامك، والصداقات التي يتم اقتراحها عليك، والإعلانات التي تراها، هي لوغاريتمات مطوّرة بذكاء؛ بحيث تتلائم مع توجهات المستخدم. واللوغاريتم ببساطة هو الخريطة التي تحدد كيف يمكن إنجاز مهمة معينة ومحددة وموضحة بدقة؛ فهو طريقة ومنهج حل مشكلة ما. يعتمد اللوغاريتم على مجموعة عمليات عقلية ورياضية، سواء كانت بسيطة أو معقدة، وتأخذ في الاعتبار قيمة محددة أو مجموعة قيم كمدخلات، لتخرج قيمة معينة أو مجموعة من القيم كمخرجات نهائية، يمكن من خلالها إصدار حكم معين أو اتخاذ قرار معين[17]. بل يمكن القول، إن اللوغاريتم هو مهارة حل المشكلات. وهو أيضاً مجموعة الخطوات التي يمكن اتخاذها لحل مشكلة معينة أو إنهاء مهمة محددة [18].

فإذا شاهدت فيديو ما على موقع ال"يوتيوب"، فإنه يبدأ في اقتراح فيديوهات أخرى حول نفس موضوع الفيديو الأول. ومع إضافة لوغاريتمات "فيس بوك" التي تحاول فهم آراء المستخدم وتقديم ما يُوافقها، فقد يتحول ال"فيس بوك" إلى ما يُشبه المرآة التي يرى فيها المستخدم صورته؛ حيث تتحكم اللوغاريتمات في محتوى «خلاصات الأخبار news deef». فمع تقليل المستخدمين تدريجياً من وجود آراء معينة باختيار عدم متابعة أصحابها، تستجيب اللوغاريتمات المصممة، وذلك لإظهار محتوى مُشابه لما يتفاعل معه المستخدمون؛ فمثلاً يرى المهتمون بشؤون العراق منشورات من أصدقائهم المهتمين بهذا الشأن، ويطّلع المهتمون بقضية التغير المناخي على نقاشات لأشخاص يشتركون معهم في هذا الاهتمام[19]. وأحد أهم استخدامات اللوغاريتمات في مواقع التواصل الاجتماعي، هو اقتراح الصداقات. فبناءً على عدد من المدخلات قد تتمثل في مكان الإقامة أو الدراسة أو العمل أو مشاركة هوايات مشتركة أو العمل على نفس شبكة الإنترنت، تبدأ اللوغاريتمات في العمل واقتراح صداقات لك على مواقع التواصل الاجتماعي تكون بالفعل لك سابق معرفة بها أو على الأقل تشاركك نفس الاهتمامات.

كما أنه يساهم في تحديد اتجاهات الرأي العام، ويظهر ذلك في خاصية Trend التي تقدمها بعض مواقع التواصل مثل "تويتر"؛ حيث يتم استخدام لوغاريتم معين يعتمد على عدد مرات ذكر القضية، والفترة الزمنية التي تمت فيها، ودرجة ارتباط المغردين بعضهم ببعض، ونسبة المحتوى الجديد الذي تم إضافته، ونسبة إعادة التغريدات التي تمت، لكي يحدد أن هذه قضية رئيسية مثارة الآن على موقع "تويتر". ومن ثم فإن اللوغاريتم هو الذي يوضح لنا ما الذي يشغل الرأي العام الآن، وما الذي يفكرون به وما هو في عقولهم؛ ومن ثم فإن اللوغاريتم قد ربط المؤشرات الكمية بالأفكار الكيفية المعبر عنها كتابياً. ونتيجةً لاعتماد اللوغاريتم مدخل "سرعة انتشار" الهاشتاج لكي يظهر في الترند؛ فإن ذلك قد يؤدي إلى عدم ظهور هاشتاجات استحوذت على

مراتب كبيرة، ولكنها تطورت خلال فترة زمنية طويلة، ومن ثم فإنه يستبعدها من Trend رغم أن عدد التغريدات بها قد يكون أكبر بكثير من هاشتاجات أخرى ظهرت في Trend، وذلك بسبب متغير سرعة الانتشار الذي يعتمده اللوغاريتم.

رابعاً: مراحل تطور الشبكات الاجتماعية - الجيل الأول .. Establishment Phase ظهر هذا الجيل مع بداية ظهور صفحات الويب web1، ورغم ضعف إمكانياتها مقارنة بالتقدم المحرز حالياً، إلا أنها كانت بمثابة مرحلة تأسيس، أكثر من كونها مرحلة انطلاق؛ حيث شهدت محاولات لإنشاء شبكات تواصل اجتماعي، باءت جميعها بالفشل. ومن أبرز الشبكات التي تكونت فى هذه المرحلة شبكة sixdegrees.com، التي منحت للأفراد المتفاعلين فى إطارها فرصة طرح لمحات عن حياتهم وإدراج أصدقائهم. وفي عام 1995 صمم "راندي كونرادز" موقع Classmates.com، وكان الهدف منه مساعدة الأصدقاء والزملاء، الذين جمعتهم الدراسة في مراحل حياتية معينة وفرقتهم ظروف الحياة العملية في أماكن متباعدة على الالتقاء واستمرار الصداقات، وكان هذا الموقع يلبي رغبة هؤلاء الأصدقاء في التواصل فيما بينهم إلكترونياً. كما تم إنشاء مواقع أخرى مثل موقع live journal، وموقع Cyworld 1999 الذى أنشئ فى كوريا، وموقع Ryze الذي كان يهدف إلى تكوين شبكات اجتماعية لرجال الأعمال لتسهيل التعاملات التجارية [20]. إلا أن هذه المرحلة لم يكتب لها البقاء بسبب ضعف الإمكانيات التي كانت تقدمها هذه المواقع لروادها، فضلاً عن الانتشار المحدود لشبكة الإنترنت حول العالم.

- الجيل الثاني.. Spread Phase جاء هذا الجيل كرد فعل على تطور صفحة الويب؛ حيث ظهر مع بداية ظهور web2، بما تتميز به من تطوير أدوات التواصل الإلكتروني سواء عبر المحادثات الفورية أو الصور أو مقاطع الفيديو. وذاع صيت برامج مثل "ياهو ماسنجر" وبريد ال"هوت ميل". وبدأت مواقع التواصل الاجتماعي في الظهور من جديد؛ حيث يعتبر الموقع الأمريكي My Space بدايةً لتدشين الجيل الثاني. ثم تتابع ظهور العديد من مواقع التواصل مثل ASmallWorld, Bebo, Diaspora, Hi5, LinkedIn, Ning, Orkut, Plaxo, Tagged, XING , IRC, Yammer، إلا أن المنافسة القوية بين الشبكات الاجتماعية أفرزت نماذج ناجحة أبرزها Facebook, Twitter, YouTube واستطاعت استغلال خصائص Web2 في إدراج عناصر متميزة بها؛ مثل خاصية الفيديو والصور والمحادثات الفورية والمشاركة الآنية للأفكار والحالات الاجتماعية. وقد حقق هذا الجيل من الشبكات الاجتماعية العديد من الإنجازات على مستوى التعارف الشخصي وتجميع البيانات والتسويق التجاري.

- الجيل الثالث.. More Connected:

ظهر هذا الجيل نتيجةً لتطور المكونات المادية والبرمجية للبنية التحتية للإنترنت، فشهد تطوير الجيل الثاني من الويب بما تميز به من ذكاء صناعي وقدرة على تبويب وتصنيف المعلومات، بالإضافة إلى تطوير المكونات المادية من خلال تقديم خدمات الجيل الثالث 3G على نطاق واسع، وزيادة سرعة الإنترنت المنزلي، بالإضافة إلى انتشار استخدام إنترنت الهاتف المحمول على نطاق واسع. واستطاعت الشبكات الاجتماعية الاستفادة من هذه المميزات والعمل على تطوير أدوات التواصل بين مستخدميها، واتسعت أسواقها وزاد عدد مستخدميها، حتى وصل عدد

مستخدمي موقع Facebook إلى أكثر من 1.2 مليار مشترك حتى عام 2013، وشهد ظهور مواقع تواصل جديدة احتلت مكانها على خريطة الشبكات الاجتماعية مثل + Google وInstagram.

وقد ازدادت أهمية الشبكات الاجتماعية في هذا الجيل، خاصةً بعد الدور الهام الذي لعبته خلال ثورات الربيع العربي 2011، فقد كانت الوسيط الرئيسي لحشد الملايين من المواطنين، والأداة الرئيسية لنشر وتنظيم المظاهرات في الشوارع والميادين، واستطاعت تهديد العديد من النظم السياسية القديمة؛ مثل نظام مبارك في مصر. وبات يتم النظر إليها من خلال النظم السياسية على أنها أحد مهددات الأمن القومي للدول؛ مما دفع العديد من النظم السياسية إلى غلق هذه المواقع أو الاكتفاء بمراقبة ما يجري عليها من أحداث، وأصبحت أداة إعلامية وإخبارية لمعرفة ونشر الأخبار لأكبر عدد من الأفراد في أقل وقت بسرعة وسهولة.

- الجيل الرابع..Application Oriented More Than Web:

لم تعد الشبكات الاجتماعية أو غيرها من المواقع حبيسة نظام الويب، بل اتجهت إلى سوق جديد واعد وقوي هو تطبيقات الهاتف المحمول Mobile App. فمع تطور المُكون المادي Hardware وانتشار الجيل الرابع من الإنترنت 4G بين المستخدمين، أصبح بالإمكان الولوج إلى الإنترنت من خلال الهاتف الذكيSmart Phone أو الحاسب اللوحي Tablet أو أجهزة التليفزيون الذكية Smart TV، أو غيرها من الأجهزة الحديثة؛ مثل نظارة جوجل أو ساعة سامسونج، وذلك بشكل أسهل وأسرع من الجيل الثالث.

وقد تميز هذا الجيل بالاعتماد على التطبيقات Applications أكثر منه على صفحة الويب؛ حيث أصبح لكل موقع إلكتروني تطبيق خاص به يمكن الولوج إليه من خلاله، يتميز بالبساطة والسرعة والتخصص في نقل المعلومات. هذا التطور المتسارع في الأجهزة الإلكترونية جعل الفرد متصلاً بالإنترنت في أي وقت وفي كل مكان، وبالتبعية ازداد ارتباطه بالشبكات الاجتماعية التي استفادت بصورة كبيرة من هذا التطور التكنولوجي المتسارع، ومن ثم تزداد تبعاتها، سواء على السياسة أو الاقتصاد أو التجارة.

خامساً: تصاعد دور الهاشتاج في مواقع التواصل الاجتماعي مثّل الهاشتاج Hashtag# ظاهرة سياسية حقيقية في الدول العربية؛ فأي تطورات سياسية أو اقتصادية أو اجتماعية أو حتى إنسانية يصاحبها دائماً هاشتاجات، إما بالتأييد وإما بالرفض. وقد اتجهت العديد من مواقع التواصل لإدخال خاصية الهاشتاج عليها؛ الأمر الذي جعلها من أكثر الأدوات استخداماً في مواقع التواصل الاجتماعي؛ حيث تضاعف عدد مستخدمي الهاشتاج عبر "تويتر"، واتجهت مواقع ال"فيس بوك" و"جوجل بلس" و"إنستجرام" لاستخدام هذه الخاصية؛ فأصبحت واحدة من أقوى أدوات التأثير داخل هذه المواقع. وقد يكمن السبب الرئيسي في توجه مستخدمي مواقع التواصل الاجتماعي نحو الهاشتاج في استهلاكهم لمختلف أدوات التواصل الموجودة حالياً - من كتابة حالة أو تعليق أو تغريدة أو مشاركة الصور والملفات Sharing- هو حاجتهم إلى أدوات تواصل جديدة تتطور بنفس السرعة التي تتطور بها التكنولوجيا؛ فكان التوجه نحو الهاشتاج. وتعتبر السمة الرئيسية فيه هي عدم وجود إدارة مركزية تتحكم في الرسائل التي يتم بثها من

خلاله؛ فالجميع لهم نفس المساحة المتساوية للتعبير عن رأيهم، ويحظون بنفس فرص الظهور أمام الأصدقاء والباحثين عن الهاشتاج؛ مما جعله وجهة لكثير من مستخدمي مواقع التواصل، غير صفحات ال"فيس بوك"، التي تعتمد على المركزية في الإدارة والتحكم.

وللهاشتاج سمات رئيسية منها:

- الانتشار السريع، وتعتبر من أهم مميزات استخدام الهاشتاج، قدرته على الانتشار السريع والوصول إلى أكبر عدد من الأفراد في زمن قياسي؛ فبمجرد إطلاق هاشتاج يحمل رسالة أو يتناول قضية أو خبر ساعة؛ فإنه ينتشر بسرعة بين مستخدمي مواقع التواصل الاجتماعي.

- مؤشر أولي لقياس الرأي العام الإلكتروني، ورغم أنه مؤشر غير دقيق إلا أنه يعكس اتجاهاً عاماً سائداً داخل فئة معينة من المجتمع في خلال فترة زمنية معينة.

- الهاشتاج المسئ هو الأسرع انتشاراً، فقد ظهرت بعض الهاشتاجات المسيئة وانتشرت أسرع من غيرها في زمن قياسي داخل مواقع التواصل.

- العمر الافتراضي للهاشتاج قصير، لأنه غالباً ما يكون رد فعل على موقف قد يتغير، أو حملة دعائية مرتبطة بفترة زمنية معينة، فالهاشتاجات تتغير وفقاً للأحداث اليومية.

- القدرة على الوصول إلى الجمهور المستهدف في الوقت الحقيقي؛ لأن الآلية التي يعمل بها الهاشتاج تتيح الوصول إلى الجمهور المستهدف. ويتم عرض الهاشتاج في نفس وقت التعبير عنه على مواقع التواصل الاجتماعي.

وكان نتيجةً لذلك أن ظهر له العديد من التداعيات، سواء الإيجابية أو السلبية أهمها:

- القدرة على خلق تعاطف دولي مع بعض القضايا المحلية، حيث يمكن للهاشتاج الذي يتناول قضايا محلية أن يحظى باهتمام وتعاطف دولي، خاصة عند كتابته بلغات أخرى غير العربية.

- تشويه الرموز السياسية؛ فتم توظيف الهاشتاج لتوجيه إساءات لبعض القادة السياسيين ورؤساء الدول والرموز، سواء كانت سياسية أو دينية أو مجتمعية.

- تنظيم مظاهرات افتراضية، من خلال استخدام الهاشتاج لعرض مطالب سياسية أو فئوية، عبر إطلاق هاشتاج ينتشر في مواقع التواصل الاجتماعي يحوي هذا المطلب.

- ظواهر اجتماعية سلبية، صاحب انتشار الهاشتاج بعض الظواهر الاجتماعية السلبية مثل استخدامه في عمليات الغش الإلكتروني أثناء الامتحانات الدراسية.

ورغم ذلك فهناك عدة استخدامات إيجابية للهاشتاج منها:

- منصة إعلامية أثناء الأحداث الكبرى؛ فقد تم توظيف الهاشتاج بصورة فعالة أثناء تنظيم كأس العام 2014، وأتاح الفرصة لمتابعة أخبار الحدث الرياضي الأهم بصورة فورية وتفاعلية.

- حملات إلكترونية للتوعية العامة؛ حيث ظهرت العديد من الحملات الإلكترونية لمواجهة ظواهر سلبية في المجتمعات؛ مثل ظاهرة التحرش وبعض الحملات التي يمكن تنظيمها لتوعية المجتمع بقضية هامة أو بسلوك معين.

- استطلاع الآراء حول قضايا مثارة، بهدف معرفة اتجاه الرأي العام نحو بعض القضايا، أو مشاركة الشباب ومستخدمي مواقع التواصل الاجتماعي في قضايا معينة أو سياسات تتبعها الدولة.

سادساً: كيف نشأت إمبراطورية ال"فيس بوك"؟

في يوم 4 فبراير عام 2004 كان "مارك زوكربرج" جالساً في حجرته بمسكن الطلبة بجامعة "هارفرد" الأمريكية، يعكف على إنشاء موقع إلكتروني، وكان لديه من البداية هدف واضح ومحدد، هو تجميع زملائه من الطلاب بعد التخرج، وإنشاء منصة إلكترونية تتيح لهم التواصل فيما بينهم وتبادل الأخبار حتى بعد التخرج.

ولعل أهم ما في تجربة ال"فيس بوك"، والذي هو أساس نجاح أي مشروع مهما كانت سذاجة الفكرة، هو وضوح الهدف وتحديده بدقة، دون تحميله أي أفكار فضفاضة أو قيم مثالية بعيدة عن الواقع. وهو ما جعل من ال"فيس بوك" منصة إلكترونية عملاقة تجمع أكثر من مليار مستخدم حول العالم، فضلاً عن التجديد في طرح الفكرة، فلم يسعَ "مارك" إلى إنشاء موقع لجذب الإعلانات كما كان معتاداً، أو عرض الأخبار، أو مشاركة الأفلام والأغاني، بل كانت فكرة مختلفة نوعاً ما، كما أنها لم تكن الأولى، بل سبقها محاولات أخرى، نجح بعضها وفشل البعض الآخر.

وقد أطلق "زوكربرج" في البداية على هذ الموقع اسم thefacebook.com وقد كان شكله بدائياً، كما يوضح التصميم التالي وهو التصميم الأولي الذي تم تصميمه عام 2004.

وتوضح الصورة التالية صفحة فريق في Facebook كما بدت عام 2005.

في عام 2006 تغير اسم الموقع ليصبح Facebook وزاد عدد المستخدمين ليشمل بينهم طلاب جامعات أخرى غير "هارفارد" ثم مدارس الثانوية، وهكذا بدت صفحة مارك زوكربرج على موقع ال"فيس بوك" عام 2006.

وفي سبتمبر 2006 كان التطور الأبرز، حين أصبحت صفحة "تغذية الأخبار "(News Feed) متوافرة، إذ تمكن المستخدم أن يرى في صفحة واحدة جامعة، ما نشره أصدقاؤه وسمح ال"فيس بوك" للأفراد الأكبر من 13 سنة للانضمام للموقع.

وفي أبريل 2008 أصدر ال"فيس بوك" أول منصة دردشة، وقد كان التطور الأبرز لل "فيس بوك" عام 2009 حيث شهد تغيراً في التصميم وإضافة خصائص جديدة من بينها زر Like للإعجاب.

أما عام 2010 فأتى ال"فيس بوك" بالإشعارات (Notifications) إلى الشريط الأعلى (Top Navigation Bar) في الموقع، عبر تصميمٍ جديد لصفحة الحساب الشخصي. وتطور التصميم الجديد، ليشمل صوراً جديدة للشخص مباشرةً تحت معلوماته الشخصية[21].

وفي سبتمبر 2011 قام ال"فيس بوك" بإصدار تحديث جديد ليدخل ضمن خصائصه "التايم لاين" "Timeline" وهي نسخة جديدة من الحائط أو "Wall" تسمح للمستخدمين بعرض

مقتطفات من حياتهم وإضافة غلاف "فيس بوك" كي يصبح على شكل كتاب وليس المشاركات الأخيرة كما كان في البداية.

وقد قام ال"فيس بوك" بتوسيع إمبراطوريته في أبريل 2012؛ حيث قام بشراء تطبيق إنستجرام "Instagram" وهى شبكة اجتماعية لتبادل الصور، بمقابل 1 مليار دولار، جزء منها يُدفع نقداً والآخر أسهماً في الشركة، مع كشف خطط إدراج ال"فيس بوك" في بورصة "ناسداك" تحت الرمز "FB" [22]، وفي مايو 2012 حدد ال"فيس بوك" سعر السهم بحوالي 28 دولار ووصل في خلال ساعات إلى 35 دولار ثم إلى 38 دولار بعد أيام، وبدأ تداول الأسهم في اليوم التالي مع نزول سعر السهم بشأن مخاوف من قدرة ال"فيس بوك" على تحقيق أرباح من الإعلانات.

وفي إطار استمرار تعظيم إمبراطوريتها؛ قامت شركة ال"فيس بوك" بشراء تطبيق المراسلات الفورية الأكثر استخداماً ال"واتس آب"، في صفقة بلغت قيمتها 19 مليار دولار عام 2014، وينص الاتفاق على أن تدفع "فيس بوك" مبلغ 4 مليارات دولار نقداً، و12 مليار دولار على شكل أسهم "فيس بوك"، وفي إطار الاتفاق انضم "جان كوم" الشريك المؤسس والرئيس التنفيذي ل "واتس آب" إلى مجلس إدارة "فيس بوك" ومنحت الشبكة الاجتماعية وحدات أسهم مقيدة بقيمة 3 مليارات دولار لمؤسسي "واتس آب" بما فيهم "كوم".

ومن الطريف أن الشاب الأوكراني "جان بورس كوم"، مخترع تطبيق "واتس آب" قد تقدم للعمل في شركة "فيس بوك" مع صديقه "بريان أكتون" عام 2007، ولكن تم رفضهما، ما دعاه للتفكير مع صديقه في إطلاق تطبيق جديد للدردشة عام 2009، وهو تطبيق "واتس آب" المجاني، الذي بدأ العمل فيه داخل منزله وعلى المقاهي. وقد كتب لشركة ال"واتس آب" النجاح منذ بداية إطلاقها، وأُقبل عليها مستخدمو شبكة الإنترنت بكثرة؛ حيث بلغ عدد المشاركين بعد 5 سنوات إلى 450 مليون مشارك، وبلغت قيمة التطبيق نحو 6.8 مليار دولار[23].

ونجح "جان كوم" مخترع تطبيق "واتس آب" في الوصول بطريقة مختلفة وشاقة لشركة "فيس بوك"، التي رفضت تعيينه لديها بالإضافة إلى أنه عانى كثيرًا في حياته الشخصية والعملية.

ولم تتوقف إمبراطورية ال"فيس بوك" عند هذا الحد، ففي يناير 2015 قامت شركة "فيس بوك" بالاستحواذ على شبكات Quickfire Networks، تلك الشركة الناشئة التي قامت بإنشاء وسيلة تسمح بعرض مقاطع الفيديو عالية الجودة باستخدام سرعة إنترنت منخفضة. ومن الملاحظ أن هذا الاستحواذ أتى بعد يوم واحد من إعلان ال"فيس بوك" أنَّ مقاطعها حصلت على أكثر من مليار مُشاهدة يومية منذ يونيو 2014. وطالما أن المستخدمين يسيرون في هذا الاتجاه، فذلك يؤكد أن الشركة تمضي على المسار الصحيح[24].

كما أعلنت شركة Wit.ai المتخصصة في تقنيات التعرف على الصوت ومعالجة اللغات الحيّة، أن "فيس بوك" استحوذت عليها بدون أن تكشف عن قيمة الصفقة؛ حيث يستخدم المطورون خدمات وتقنيات Wit.ai من أجل الحصول على بيانات مهيكلة من الكلام المنطوق. ويحدث الأمر ببساطة؛ حيث ترسل العبارة المنطوقة إلى خدمة Wit.ai والتي تقوم بتحويلها إلى JSON يمكن استخدامه في تطبيقك. ولعله من غير الواضح بعد ماذا تريد "فيس بوك" من هذه الشركة،

ولكن هناك على الأقل احتمالان: الأول هو أن تطلق "فيس بوك" مستقبلاً خدمة محرك بحث صوتية أو مساعد مشابه ل Siri الموجودة على هواتف ال"آي فون" وتدمجه ضمن شبكتها الاجتماعية. والثاني هو استخدامها كأداة إدخال لجهاز الواقع الافتراضي من oculus ومن أجل استخدام الصوت في التطبيقات على النظارات الذكية حيث لاتزال تفتقر لأدوات الإدخال [25].

وفي إطار سعيها لنشر خدماتها حول العالم، ووصولها إلى المناطق النائية والريفية والتي يصعب تقديم خدمات الإنترنت فيها، ترعى شركة ال"فيس بوك" العديد من المشروعات التي تقدم خدمات الإنترنت بصورة مجانية، ومن الخدمات الرئيسية التي تسعى شركة ال"فيس بوك" إلى تقديمها هي خدمة الإنترنت المجاني عبر منظمة Internet.org غير الربحية التي تم إطلاقها أول مرة في عام 2013 وهى تهدف لنشر خدمة الإنترنت المجاني في المناطق النائية والفقيرة حول العالم من أجل مساعدة سكانها في التواصل مع الآخرين والتمتع بالإنترنت في كافة مجالات حياتهم، وقد توصلت شركة "فيس بوك" لاتفاق مع "ريلاينس كوميونيكيشن" في الهند لتوفير خدمات الإنترنت على الهواتف المحمولة مجاناً في فبراير 2015، لتكون الهند بذلك أول دولة في قارة آسيا تشملها خدمة "إنترنت دوت أورج" التابعة ل "فيس بوك". وقد دشنت "فيس بوك" خدمات مماثلة في زامبيا وتنزانيا وكينيا وغانا وكولومبيا [26].

وقد أعلنت شركة ال"فيس بوك" في وقت سابق عن نيّتها لتقديم خدمات الإنترنت بصورة مجانية عبر أقمار صناعية صغيرة؛ تقوم ببث خدمات الإنترنت في المناطق النائية عبر محطات أرضية، ولكن على ما يبدو أن الشركة قد تخلت عن هذا المشروع بسبب التكاليف الباهظة المترتبة على المشروع. وقد كانت الشركة قلقة من أنها لن تكون قادرة على استرداد تكاليفها من المشروع.

ورغم محاولات شركة ال"فيس بوك" الاستحواذ على العديد من الشركات والتطبيقات لزيادة وتوسعة إمبراطوريتها، فإن هناك شركات أخرى حاولت الاستحواذ عليها وفقاً لموقع businessinsider إلا أنها جميعاً باءت بالفشل، ولعل من أبرز هذه المحاولات[27]:

في 2004 وبعد تأسيس موقع ال"فيس بوك" بأربعة أشهر فقط، عُرض على "مارك" استثمار قيمته 10 مليون دولار من مستثمر لم يفصح عن اسمه، ولم يبدِ "مارك" لهذا العرض أي اهتمام.

واحدة من إحدى محاولات الاستحواذ على شركة ال"فيس بوك" كانت من الموقع الاجتماعي Freindster، وهو موقع كان منافساً حينها ل "فيس بوك"، أطلق عام 2002 وقلت شعبيته مع ظهور شبكات اجتماعية أفضل تصميماً، حيث يقول مؤسس موقع Freindster “لقد وجدت شركة صغيرة، وكنّا سنشتريها بالفعل وكان مشروعاً ناشئاً ولم يسمع عنه أحد – في ذلك الوقت – شركة تسمى The Facebook”، بالفعل كانت ستتم الصفقة بشراء "فيس بوك" ولكن Friendster انشغلت بجولة أخرى من الاستثمار وفجأة انطلق "فيس بوك" وخسرت Frienster آخر أمل لها لتكمل بين العمالقة[28].

في صيف 2004 انتقل "مارك" ورفقائه في السكن لاستئجار منزل ب "بالو ألتو" ب "كاليفورنيا"، لم يمضِ وقت حتى أرسلت "جوجل" اثنين من مديريها التنفيذين ليناقشا مع "مارك" إمكانية شراكة العمل مع "فيس بوك" أو حتى شراؤه إن أمكن، لم يسفر اللقاء عن أية نتائج، وقد عادت المحاولات عام 2007 ولكن بطريقة أخرى، حاولت "جوجل" فيها عقد صفقة لاستخدام الإعلانات على "فيس بوك"، ولكن لم تفلح هي الأخرى، محاولتها الأخيرة أتت بعرض 15 مليار دولار لشراء "فيس بوك" ولكن هذه الصفقة أيضاً لم تتم.

وفي ربيع 2005 طبقاً لحديث "فيس بوك" مع جريدة ال"واشنطن بوست" فقد عرضت شركة Viacom استثماراً يقدر ب 75 مليون دولار لشراء شركة "فيس بوك"، وفي نفس الفترة كانت أرباح "فيس بوك" 35 مليون دولار، ولكنها لم تبدِ اهتماماً بالعرض، تلاه في أوائل عام 2006 لقاء ل "مارك" مع مدير MTV شرح فيه "مارك" نظريته بأن الشركة تُقدر ب 2 مليار دولار على الأقل، لم يمضِ من الوقت إلا أسبوعان حتى أرسلت 1.5 مليار دولار (800 مليون دولار مقدم وبقية الدفع على مراحل)، كانت "فيس بوك" على وشك أن تُباع حتى بالغ "مارك" في زيادة السعر مما أصاب مديري شركة Viacom بالغضب، وفشل الاتفاق ولم تحاول بعدها مرة أخرى.

في صيف 2006 حاولت "ياهو" شراء "فيس بوك" بمليار دولار، ومعظم مستثمري "فيس بوك" كان لديهم القابلية للبيع ولكن "فيس بوك" كانت على وشك إطلاق تصميم جديد واعتقد "مارك" أنه لو نجح فإن شركة "فيس بوك" ستستحق أكثر من تلك القيمة.

في منتصف عام 2006 قرر المدير التنفيذي لشركة Aol "جوناثان ميللر" شراء شركة "فيس بوك"، وكانت خطته لتوفير مبلغ مليار دولار من أجل شراء "فيس بوك" هي بيع MapQuest وTagic "مشاريع تابعة للشركة"، وأقنع شركة Time inc ببيع IPC ولكن لم ينجح في شراء "فيس بوك".

"لما لا نشترِ "فيس بوك" ب 15 مليار دولار" كان هذا عرض المدير التنفيذي ل"مايكروسوفت" على "زوكربرج" عام 2007، لإبعاد "فيس بوك" عن أيدي "جوجل"، عرض "ستيف بالمر" هذا العرض على "مارك"، ومن الغريب في هذه الصفقة أن هذه الأموال كانت فقط لشراء جزء من "فيس بوك" بعدها سيكون ل "مايكروسوفت" إمكانية شراء 5% من قيمة "فيس بوك" كل 6 أشهر، أي أن شراء كامل الشركة سيستغرق من 5 إلى 7 سنوات.

ولعله من المنطقي أن تبوء كل هذه الصفقات بالفشل، فحتى يوليو 2014 كانت القيمة السوقية لشركة ال"فيس بوك" 190 مليار دولار، وتجاوز سعر السهم حدود 75 دولار، كما أن هناك سبباً آخر لزيادة القيمة السوقية لشركة ال"فيس بوك"، ألا وهو سياستها الإعلانية المتعددة، فبفضل عدد مشتركيها الذين وصلوا إلى 1.44 مليار مشترك نشط في مارس 2015، أصبح ال"فيس بوك" أكبر تجمع إلكتروني على مستوى العالم، ولعل الميزة التنافسية لشركة "فيس بوك" أن أكثر من 30 مليون شركة ناشئة لديها صفحات على الموقع، هذه الشركات مع اختلاف رأس مالها تسعى للإعلان عن نفسها في أكبر موقع تواصل اجتماعي في العالم، ولعل الشركات الصغيرة والمتوسطة هي المستفيد الأكبر من إعلانات ال"فيس بوك" المنخفضة التكلفة نسبياً حيث تتراوح أسعار الإعلانات من 5 إلى 50 دولاراً، هذا فضلاً عن دقة تحديد الجمهور المستهدف، حيث يستطيع

محل للمأكولات أن يستهدف سكان منطقة محددة، وليكن مثلاً سكان شارع فيصل بالجيزة الذين تتراوح أعمارهم بين 15 – 45 عاماً، فتظهر إعلاناته فقط لهذا الجمهور.

الفصل الثالث: التداعيات المترتبة كيف أصبحت شبكات التواصل مصدر تهديد للأمن القومي للدول؟

إن تزايد استخدام الشبكات الاجتماعية، سواء مواقع الإنترنت أو تطبيقات الموبيل، أفرز عدداً من التداعيات التي ألقت بظلالها، سواء على المواطن أو الدولة أو الشبكات الاجتماعية ذاتها، ولعل أهمها:

أولاً: التداعيات المترتبة على تزايد استخدام مواقع التواصل الاجتماعي:

- نهاية عصر الخصوصية:

فالبيانات الشخصية والدقيقة أصبحت متاحة ومكشوفة، بل إن حياة الأشخاص أصبحت موثقة عبر حساباتهم على الشبكات الاجتماعية؛ فكل ما يفكر به الفرد ويكتبه ويشاركه مع أصدقائه أو الصفحات التي يشترك فيها، أصبح محل نقاش جماعي من كل أصدقائه. وأصبحت شركات الشبكات الاجتماعية تمتلك قواعد بيانات كاملة عن أدق تفاصيل حياة مشتركيها. كما أن الأفراد الغير مشتركين في مثل هذه المواقع لم يعودوا في مأمن منها؛ فيكفي أن يكون لديهم أصدقاء مشتركون في الشبكات الاجتماعية حتى تتم معرفة معلومات شخصية عنهم، وذلك من خلال بعض تطبيقات الهواتف الذكية المستخدمة للتواصل الاجتماعي مثل What'sApp, Viber, WeChat, Line, وغيرها من مئات التطبيقات التي تتطلب إذناً من المستخدم للولوج إلى كافة البيانات الشخصية الخاصة بالأرقام الموجودة على هاتفه المحمول. بل تم تطوير تطبيقات في ظاهرها ألعاب للترفيه والتسلية، وفي حقيقتها برامج للتجسس وجمع المعلومات.

حيث كشف تقرير نشرته صحيفة "الجارديان" البريطانية، أن وكالة الأمن القومي الأمريكية NSA تقوم بتطوير تقنيات تسمح لها باستغلال تطبيقات الهواتف الذكية للوصول إلى معلومات خاصة بالمُستخدمين، ومن أبرز هذه التطبيقات وأكثرها انتشاراً، تطبيق الطيور الغاضبة Angry Birds، وهي لعبة ذائعة الصيت على الأجهزة المحمولة واللوحية [29]. كما سرّب "أدورد سنودن" –المتعاقد السابق مع وكالة الأمن القومي الأمريكي- وثائق تؤكد استهداف وكالة الاستخبارات الأمريكية CIA بيانات الهاتف المحمول للمُستخدم؛ وذلك لجلب معلومات عن الإرهابيين وأهداف استخباراتية أُخرى؛ حيث أنفقت ما يزيد على مليار دولار لصالح برامج التجسس الخاصة باستهداف الهواتف الذكية[30].

- تزايد سيطرة الدول:

يرى البعض أن الجيل القادم من الشبكات الاجتماعية سيكون لصالح الأفراد أكثر من الدول، وهو اعتقاد ليس صحيحاً؛ فقد كشفت تسريبات "سنودن" الدور الذي لعبته الحكومة الأمريكية في التجسس على عدد كبير من الأفراد حول العالم وليس داخل الولايات المتحدة فقط، بالإضافة إلى البرامج الحكومية المتخصصة في مراقبة الشبكات الاجتماعية. وقد تزامن ذلك مع اتجاه معظم الدول إلى مراقبة شبكاتها الاجتماعية، خاصةً بعد الدور الذي لعبته مواقع التواصل خلال ثورات الربيع العربي، وسعيها لمراقبة الناشطين السياسيين، وقيام بعض الدول بإنشاء كتائب إلكترونية وظيفتها بث رسائل وأفكار تخدم نظمها السياسية عبر الشبكات الاجتماعية؛ فالدول

لن تتهاون في أمنها القومي؛ خاصةً بعد أن أصبحت الشبكات الاجتماعية مصدر تهديد لها، وهو ما سيضعها في موضع صدام إلكتروني مع مختلف مستخدمي الشبكات الاجتماعية، وقد يأخذ التهديد أحد الأشكال التالية:

- الاحتجاج الإلكتروني: في هذه الحالة يتم استخدام الشبكات الاجتماعية باعتبارها وسيطاً للتعبئة والحشد للاحتجاج على سياسات أو خدمات مدنية؛ حيث تبدأ العديد من الحملات الإلكترونية بعرض مطالب تهم عدداً كبيراً من المواطنين داخل الدولة، بما يساهم في زيادة عملية الترويج الإلكتروني لهذه المطالب. وإذا لم تتعامل الدولة بجدية مع هذه المطالب، فإنها تجد طريقها للتصعيد سريعاً، فتتحول خلال أيام قليلة إلى احتجاجات أو إضرابات فئوية.

- المظاهرات الافتراضية: يتم تنظيم المظاهرات الافتراضية من خلال الاتفاق على موعد محدد وهاشتاج محدد على صفحات "تويتر" أو ال"فيس بوك"؛ يتجمع عليه أكبر عدد من المشتركين في لحظة معينة؛ لعرض مطالب ذات طبيعة سياسية. ويتوجب على الدولة التعامل مع الموقف إما من خلال الاستجابة المنطقية لمطالب المظاهرة، أو غلق هذه الصفحات ومحاصرة انتشارها؛ منعاً لانتقال المظاهرة من الفضاء الإلكتروني إلى الميدان.

- تشويه الرموز السياسية: ويقصد به تشويه الرموز السياسية سواء كانت شخصيات أو دول أو مؤسسات من خلال الإنترنت، خاصة بعد الاستخدام الفعّال لخاصية "الهاشتاج" بموقع "تويتر"، حيث يتم استخدامه من قبل التيارات الفكرية في حروبهم السياسية ومعاركهم الانتخابية.

- غلبة الطابع الأمني:

أحد السمات الرئيسية للجيل الجديد من الشبكات الاجتماعية هو غلبة الطابع الأمني عليها، بسبب نجاح هذه المواقع في تهديد أمن الدول. وبدلاً من الاتجاه لغلق هذه المواقع كما كان قديماً، ستعمل الدول على إنشاء كتائب إلكترونية، يكون هدفها الدفاع عن مصالح النظام عبر الشبكات الاجتماعية.

- تواجد متزايد للحركات الإرهابية:

لعل أبرز الملامح الرئيسية التي تميز بها الجيل الجديد من الشبكات الاجتماعية، هو تزايد وجود الحركات الإرهابية عليها؛ التي تستخدمها كأداة إعلامية وتجنيدية في نفس التوقيت، من خلال بث أفكارها وأخبارها عبر الشبكات الاجتماعية. وهو ما اعتمدت عليه مثلاً "داعش" في خلق صورة ذهنية لها لدى الرأي العام العراقي والدولي؛ من خلال عرض صور لمجازر إنسانية ارتكبتها، مما سهّل عليها دخول بعض المناطق الجغرافية دون مقاومة تذكر، بسبب الانطباع الذي تم ترسيخه عنها من خلال الشبكات الاجتماعية.

وتستخدم الحركات الإرهابية الشبكات الاجتماعية عادةً للتنقيب عن المعلومات، والحصول على التمويل والتبرعات وعملية التجنيد والحشد لأتباعها، وكذلك لتحقيق الترابط التنظيمي بين الجماعات داخلها وتبادل المعلومات والأفكار والمقترحات والمعلومات الميدانية حول كيفية إصابة الهدف واختراقه، وكيفية صنع المتفجرات والتخطيط والتنسيق للعمل الإرهابي.

- عدم القدرة على الخروج من الشبكات:

واحدة من خصائص الشبكات الاجتماعية القادمة هي عدم قدرة مستخدميها على الخروج منها؛ فقد خلقت هذه الشبكات حاجات Needs لدى مستخدميها، سواء من خلال متابعة الأخبار أو محادثة الأصدقاء أو التسوق أو غيرها من الحاجات اليومية التي أصبح مستخدم الشبكة الاجتماعية غير قادر على الاستغناء عنها. حتى إذا قرر الخروج منها، فالبيانات الشخصية لن تُمحى، وبمجرد عودته إليها مرة أخرى سيجد جميع بياناته دون تغيير. كما تعمل شركات الشبكات الاجتماعية مثل "فيس بوك" و"جوجل" على توسيع سوق مستخدميها؛ من خلال توفير خدمات الإنترنت في كل مكان حول العالم عبر أقمار صناعية وطائرات بدون طيار، مما يجعل هذا النوع الجديد من الشبكات الاجتماعية يطارد غير المستخدمين في كل مكان.

- تطوير أدوات تحليلية:

تميز الجيل الجديد من الشبكات الاجتماعية بتطوير أدوات تحليلية، تساعد على فهمٍ أفضل للتفاعلات الدائرة على هذا النوع من المواقع؛ من حيث عدد المستخدمين الناشطين، وأوقات الذروة التي يمكن فيها نشر حالة Statues أو مشاركة ملفات، والنسب الإحصائية لزوّار المواقع المعلن عنها على الشبكات الاجتماعية، والتوزيع الجغرافي لهم، وأوقات ومدة تواجدهم على الموقع، وتقديم رسوم بيانية توضح تطور التفاعلات على صفحات التواصل الاجتماعي خلال فترة زمنية معينة. بالإضافة إلى تطوير أدوات أخرى للمعلنين عليها؛ حيث يقدم موقع ال"فيس بوك" خدمات تساعدهم على استهداف جمهورهم بصورة أدق، تصل لحد استهداف جمهور معين في منطقة أو شارع محدد.

- تطوير أدوات تواصل جديدة:

مثّلت مواقع التواصل في الجيل الثالث والرابع نافذة إعلامية بديلة لإعلام الدولة أو إعلام الشركات؛ حيث أصبح هناك إعلام للمواطن، يصنعه وينتقل إليه، ومن المتوقع أن تزداد كثافته في المرحلة المقبلة، ولكن هذه الزيادة ستكون بشكل مختلف، فمن المتوقع زيادة مساحة الفيديوهات والصور التي تُمحى بعد 10 ثوانٍ من مشاهدتها فيما يعرف ب Snapchat، وهو ما يساعد على تلافي بعض عيوب الجيل الثاني خاصة فيما يتعلق بالصور والفيديوهات غير اللائقة التي يشاهدها بعض المستخدمين.

بالإضافة إلى تطوير أدوات جديدة للتواصل الاجتماعي من خلال النظارات الذكية والساعات الذكية، وتضمين خصائص جديدة للتراسل الفوري وتبادل المعلومات بين الأصدقاء، فضلاً عن تزايد سوق مقاطع الفيديو، حيث يحتل موقع Youtube الصدارة بين مختلف مواقع التواصل الاجتماعي لتميزه في المحتوى المرئي، ويتجه الأفراد إلى الفيديو لما يتميز به من إثارة في عرض المعلومات. وسوف يزداد هذه الاتجاه في المستقبل القريب.

- مؤشر لحالة سوق العمل والرضاء الوظيفي:

مع ظهور نوع جديد من الشبكات الاجتماعية يتمثل في الشبكات المهنية Professional Networks، من المتوقع أن يكون لها تأثير مباشر على العمال وأصحاب العمل؛ وذلك من خلال

تغيير الآلية التي تعمل بها سوق العمل حالياً، إذ يمكن أن تحل الصفحات الشخصية على موقع Linked In محل السيرة الذاتية التقليدية، وأن يجد كثير من المتخصصين مثل القادة العسكريين وظائف لهم بعد التقاعد عبر التواصل مع زملائهم من خلال موقع Hirepurpose، وأن يتمكن الأطباء من تحقيق التواصل الفعال بينهم والحصول على وظائف أفضل من خلال موقع Healthtap وموقع Sermo، وسيجد الأكاديميون مجالاً لنشر أوراقهم البحثية وتبادل المعرفة العلمية فيما بينهم من خلال موقع Academia أو موقع Researchgate.

ولعل لهذه الشبكات المهنية خصائص معينة، نتيجة لتخصصها الدقيق، واهتمامها ببعد حيوي يتعلق بعمليات التوظيف والتشغيل، يُتوقع أن تجد صدىً وردّ فعل سريع لدى أصحاب العمل والعمال، وذلك للأسباب التالية:

1 - تسهيل الحصول على الوظيفة الملائمة والموظف المناسب.

2 - تجمُع لأصحاب المهن والوظائف المتشابهة، وتبادل الخبرات بينهم.

3 - تعطي انطباعاً عن حالة العمل في دولة ما، من حيث أكثر القطاعات جاذبية للعمل وأكثر الوظائف توافراً.

4 - معرفة مستوى الخبرات الوظيفية داخل الدولة، والمهارات التي يتمتع بها العمال.

5 - توضح اتجاهات الاستثمار في البلد، من خلال معرفة أكثر الوظائف التي يتم البحث عنها.

6 - معرفة أكثر القطاعات الوظيفية إرضاءً للموظفين، سواء من حيث المرتبات أو بيئة العمل.

7 - تحديد أكثر الوظائف التي ينفر منها العمال، ويتجهون للبحث عن وظائف أخرى.

8 - تعكس درجة الاستقرار الوظيفي داخل الدولة من خلال معرفة حالات البحث عن الوظائف الجديدة.

9 - معرفة الاتجاهات العامة في الدولة حول سبب قيام الموظفين بتغيير وظائفهم.

10 - تسويق المنتجات وسهولة الحصول على العملاء المستهدفين.

وتعتبر شبكة "لينكد إن" التي تم إنشاؤها في 5 مايو 2003، من أكبر المواقع المهنية انتشاراً حول العالم، وأكثرها عدداً، حيث يصل عدد أعضاءها إلى 364 مليون عضو في حوالي 200 دولة حول العالم وفقاً لإحصاءات الشبكة الرسمية حتى يوليو 2015، وثمة أكثر من 4 مليون شركة تمتلك صفحات لها على "لينكد إن". كما أنها متوافرة ب 23 لغة، ولديها أكثر من 6000 موظف في 30 مدينة حول العالم.

وقد كشفت دراسة أجرتها شبكة "لينكد إن"، عن أن يوم الأربعاء الموافق 21 يناير 2015 على سبيل المثال شهد نشاطاً أعلى من المتوقع من قبل المهنيين الأعضاء على الموقع، وذلك بهدف تحديث ملفاتهم الشخصية، والبدء بتطبيق خططهم المهنية للعام الجديد.

ومعلوم أن شبكة "لينكد إن" تتيح للأعضاء خدمة البحث عن الشركات والوظائف التي يرغبون في الحصول عليها، ومشاهدة قراءات وإحصاءات حول هذه الشركة. وتلك الإحصائيات قد تشمل

نسبة الموظفات النساء مقابل الموظفين الرجال في الشركة، وموقع الشركة الرئيسي وأماكن مكاتبها، أو قائمة بموظفيها السابقين والحاليين.

وحتى يمكن الوقوف على أهمية هذه الشبكة، يمكن تناول حالة دولة الإمارات وفقاً لتقرير صدر من مُلّاك شبكة "لينكد إن" أوائل العام الجاري، إذ تجاوز عدد مستخدمي الشبكة في دولة الإمارات أكثر من مليون مستخدم. وأوضح التقرير "حالة الرضا وعدم الرضا" بين الموظفين داخل الدولة خلال عام 2014، حيث قسمهم إلى قسمين: الموظف النشيط، وهو الذي يسعى للترقي الوظيفي، والموظف السلبي، وهو الراضي بعمله الحالي دون رغبة في تحدٍ جديد، وكانت نتيجة التقرير كالتالي:

30% من الموظفين "راضون جداً" عن عملهم، وأغلبهم من الموظفين السلبيين.

47% من الموظفين "راضون إلى حد ما" عن عملهم، وأغلبهم من الموظفين الناشطين.

14% من الموظفين "غير راضين" عن وظائفهم، وأغلبهم من الناشطين.

7% من الموظفين "غير راضين إلى حد ما" عن عملهم، وأغلبهم من الناشطين.

3% من الموظفين "غير راضين تماماً" عن عملهم، وكانوا جميعاً من الناشطين.

وتعد الشبكات المهنية في الواقع جزءاً من الشبكات الاجتماعية، بما تقدمه من مزايا، وبما تحتويه من مخاطر. ولكن التحدي الرئيسي الذي تطرحه الشبكات المهنية، أنها تجعل القطاعات المتخصصة داخل الدولة أكثر انكشافاً، ليس فقط أمام الشركات والمنظمات الدولية، بل أمام الباحثين والمهتمين بهذه القطاعات.

ومع تواجد شبكات مهنية للأطباء والعسكريين، واحتمالية ظهور شبكات أخرى متخصصة تضم المهاجرين من العمال، أو الباحثين عن هجرة إلى الخارج، أو غيرها من الشبكات التي يمكن أن تظهر، فإنها تقدم تقريراً توضيحياً عن حالة هذه القطاعات داخل أي دولة، وهو ما يؤثر مباشرة على صورتها في الخارج.

ولهذا يجب التعامل مع هذا النوع من الشبكات المهنية بخصوصية عالية؛ ففي حالة أنه أظهر قطاعٌ معينٌ أداءً سيئاً عبر الشبكات المهنية، ينصح بالقيام باستطلاع رأي لمعرفة مدى مصداقية هذا الأداء، ونشر نتائجه إذا كانت في صالح تحسين صورة هذا القطاع. كما أنه يجب النظر في إمكانية خلق قنوات تواصل بين الموظفين وأصحاب العمل عبر هذه الشبكات حتى لا يكون المؤشر النهائي مضللاً. وفي حالات محددة قد يتطلب الأمر مراقبة القطاعات التي لها شبكات مهنية جيداً، ومعرفة المشكلات التي تواجه العمال والموظفين، والعمل على حلها بصورة سريعة.

ثانياً: التداعيات المترتبة على تزايد استخدام تطبيقات الموبيل للتواصل الاجتماعي أصبحت تطبيقات التواصل الاجتماعي - سواء التي تعتمد على البريد الإلكتروني أو أرقام الهاتف المحمول في التواصل بين الأفراد - ظاهرة مقلقة نتيجة لكثرة عدد هذه التطبيقات وتزايد مستخدميها بصورة كبيرة؛ لدرجة أنه أصبح من الصعب حصر جميع التطبيقات التي تعتمد على أرقام الهاتف في التواصل. بل أن بعضها يتنافس في تقديم خدمات مدفوعة بصورة مجانية لأعضائها حتى

تستحوذ على نصيب لها من سوق التواصل الاجتماعي. ومن أمثلة ذلك منح بعض المستخدمين دقائق دولية مجانية لمجرد اشتراكهم في التطبيق، أو قيامهم بدعوة أحد أصدقائهم للاشتراك فيه.

ومن أمثلة هذه التطبيقات الواتس أب وفايبر ولاين وغيرها، وجميعها تعتمد على أرقام الهاتف المحمول ويمكن تعريفها بأنها "برامج يتم تحميلها بصورة مجانية أو مدفوعة عبر منصات تحميل التطبيقات مثل "جوجل بلاي" أو "أبل ستور" أو "أمازون" أو "مايكروسوفت فون"، وتعتمد في عملية التواصل فيما بينها على رقم الهاتف المحمول الخاص بالمستخدم والمتصل بالإنترنت، وتستطيع هذه البرامج أن تصل إلى بيانات المستخدم على الهاتف، سواء كانت صور أو رسائل أو بيانات اتصالات، وأن تتعرف على أماكن تواجده، وتحتفظ بسجلات الدردشة الخاصة به".

ونتيجة لرخص تكلفة الحصول على هذه التطبيقات أو انعدام تكلفتها في بعض الأحيان، وانتشارها بين عدد كبير من المستخدمين، بدأت تظهر بعض المخاوف الأمنية تجاهها. هذه المخاوف تتمثل في الطرق التي يمكن أن تستخدم بها الجماعات المعارضة والحركات الإسلامية والجهادية هذه التطبيقات في التواصل فيما بينها لتحقيق أهدافها. وليست المخاوف فقط فيما يتعلق بانعدام خصوصية المستخدمين، من خلال قيام هذه التطبيقات بالوصول إلى المعلومات والبيانات الشخصية وسرقتها لتحقيق مكاسب مادية من خلال نظام الإعلانات أو بيعها لبعض الشركات.

توفر هذه التطبيقات عدة مميزات تشجع على تزايد مستخدميها، فبغض النظر عن رخص تكلفة الحصول عليها أو توفرها بصورة مجانية من الأساس، وما تتيحه من إمكانية إجراء مكالمات صوتية حيّة أو رسائل صوتية مسجلة أو رسائل نصيّة أو فيديوهات وصور، إلا أنها توفر عدداً من المميزات الأخرى أهمها:

- وسيط سهل وسريع لتبادل المعلومات والأخبار والصور بقدر معين من الخصوصية، فهي ليست كصفحات التواصل الاجتماعي التي يطّلع عليها جميع الأفراد ويمكن دراستها وتحليلها ومراقبتها، حيث يطّلع على المعلومة فقط الشخص الذي تم إرسال هذه المعلومة إليه.

- وصول المعلومة للشخص المستهدف تحديداً وليس لجمهور عام قد يكون منهم المستهدفون وقد لا يكون، وذلك من خلال الاعتماد على أرقام الهاتف المعروفة مسبقاً للأفراد وإرسال الرسائل النصية لهم مباشرة.

- سرعة الاطلاع على الأخبار والمعلومات، فعدد كبير من الأفراد يمتلكون هواتف ذكية متصلة بالإنترنت.

- إمكانية إنشاء "تطبيقات سرية" أو تطوير تطبيقات معروفة، للتواصل بين مجموعة معينة من الأفراد فيما بينهم بصورة تصعّب مراقبة الأجهزة الأمنية لها.

ورغم تعدد الاستخدامات الإيجابية الخاصة ببرامج التواصل المجاني، سواء في تحقيق التواصل بين الأفراد داخل وخارج الوطن دون تكلفة حقيقة تذكر، أو استخدامها في الحملات الإعلانية والترويج للخدمات والمنتجات، أو إرسال عِبر وعظات دينية، أو التنسيق بين مجموعات العمل

المشتركة، أو في عمل حملات لتجديد الولاء والانتماء لقادة الدولة وحكامها، إلا أن هناك أنماطاً أخرى لاستخدامات تطبيقات الموبيل للتواصل الاجتماعي قد تتسبب في إزعاج أجهزة الأمن، وقد تكون هذه الاستخدامات المحتملة هي:

- عملية التعبئة والحشد: وذلك من خلال تبادل المعلومات الخاصة بعمليات التجمع أو التجمهر والتظاهر أو حشد رأي عام ضد الحكومة أو ترويج إشاعات حول النظام الحاكم أو غيرها من الأكاذيب.

- جمع التبرعات: فقد تستخدم الحركات الإرهابية وكذلك المتطرفون برامج التواصل المجاني لجمع تبرعات لبعض الأنشطة التي يقومون بها من خلال أنصارهم.

- التواصل السري بين الأفراد: من خلال استحداث برنامج سري يعمل على سيرفرات داخلية يحقق لأفراد المجموعة التواصل السري بينهم، أو من خلال تطوير برامج موجودة بالفعل واستخدامها أيضاً للتواصل السري بعيداً عن أجهزة الأمن.

ومن ثم، فإن ظاهرة تطبيقات الموبيل المجانية للتواصل الاجتماعي عبر رقم الهاتف المحمول تتزايد وتتسارع، ولم تتضح بعد "بصورة كاملة" كافة أبعادها وتداعياتها، وتبقى ظاهرة جديرة بالدراسة، لمعرفة هل يمكن أن تشكل تهديداً للأمن القومي للدول؟ أو وسيطاً يمكن للجماعات المعارضة والإرهابية استخدامه في عمليات التنسيق والتخطيط بعيداً عن الأجهزة الأمنية؟.

نتيجةً لاتجاه الصراع الدولي حول الموارد والمصالح والقيم، نحو الاعتماد المتزايد على تكنولوجيا الاتصال والمعلومات، أصبح الفضاء الإلكتروني ساحة جديدة للصراع بشكله التقليدي، ولكنه ذو طابع إلكتروني يتجاوز الحدود القومية وسيادة الدول. ويسعى كل طرف من طرفي الصراع إلى تحقيق أكبر مكاسب، وإلحاق أكبر قدر من الخسائر بالطرف الآخر. ويتميز الصراع الإلكتروني بأن به تدميراً لا يصاحبه دماء أو أشلاء، ويتضمن التجسس والتسلل ثم النسف، لكن لا دخان ولا أنقاض ولا غبار. ويتميز أطرافه بعدم الوضوح، وتكون تداعياته خطيرة سواء عن طريق تدمير قواعد البيانات الموجودة على الإنترنت ونسفها، أو قصفها بوابل من الفيروسات، أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة للنيل من سلامة المواقع الإلكترونية وقواعد البيانات. وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت، ويسهل تعلم كيفية استخدامها؛ ونتج عن ذلك ظهور شكل جديد من الحروب، يكون في وسط الشعوب، بعيداً عن الساحات التقليدية للصراع الدولي، هذا الشكل هو "الحرب الإلكترونية".

أما فيما يتعلق بحروب مواقع التواصل الاجتماعي في نطاق حروب الجيل الرابع، فقد حدث تغيّر كبير في طبيعة الأطراف المتحاربة، فلم تصبح بعض الدول تستخدم جيوشاً نظامية ضخمة. وهكذا لم تصبح الدولة فقط هي صاحبة قرار الحرب، بل أضحت جماعات صغيرة من الأفراد المتشابهين فكرياً يجمعها تنظيم واضح، قادرة على اتخاذ قرار خوض الحرب. وهذا النوع من الحرب يرتبط بشنّ حرب ضد الدولة المستهدفة في مجالات شتى، وليس المجال العسكري فقط، إذ تعتمد بصورة أكبر على الحروب الاقتصادية والمالية والمعلوماتية وغيرها. كما أنها ترتكز على إقامة تحالفات وجماعات وشبكات إجرامية، بل وحتى أفراد لا تجمعهم بالضرورة مصلحة سوى إسقاط الدولة المستهدفة[31].

وقد جاءت حروب مواقع التواصل الاجتماعي لتصبح أحد أركان حروب الجيل الرابع؛ بما تميّز به من خصائص مثل: تغيّر طبيعة الخصوم، والأهداف، والأسلحة، والفاعلين الرئيسيين في هذه الحرب؛ حيث لا تستهدف هذه الحرب تحقيق نصر عسكري بقدر تحقيق نصر سياسي معنوي، يستهدف كسر الإرادة، ورفع تكلفة الخصم باستمراره في صد هذه الهجمات، بشكل يسئ إلى صورته التقليدية المحفورة في الأذهان، ويخصم من رصيده المجتمعي لدى الأفراد، ويُنفر منه التابعين له.

وفي ذلك يتم استخدام أسلحة غير تقليدية تتلائم مع الطبيعة الجغرافية الافتراضية للمكان؛ حيث الفضاء الإلكتروني بساحاته الممتدة، وخصائصه الفريدة، وأدواته المتغيرة بفعل التكنولوجيا؛ حيث لا توجد حدود بين الدول، ولا توجد مساحات بين العام والخاص، أو الرسمي وغير الرسمي. فالتقاطعات مشتركة بين الجميع، سواء كانوا أفراداً أو دولاً أو مؤسسات أو تنظيمات، ولا توجد سلطة قانونية تحكم وتنظم وتشرع وتقرّ، وإن كانت فهي موجودة على استحياء، يمكن أن تنطبق على البعض ولكنها لا تنطبق على الكل.

وفي هذا الإطار تأتي حروب مواقع التواصل الاجتماعي تحت مظلة حروب الشبكات Netwar، والتي تستهدف البنية الاجتماعية للدولة أكثر من أمنها التقليدي.

وهي غير الحروب السيبرية Cyberwar التي تركز على مفاهيم الأمن التقليدية من خلال الفضاء الإلكتروني، وتقترب من العمل العسكري المسلح من خلال استخدام أسلحة الفضاء الإلكتروني التقليدية بما فيها من اختراق الشبكات وتدمير المعلومات وسرقتها وتضليلها، وشنّ هجمات لقطع خدمات الإنترنت، أو تدمير منشآت حيوية كمحطات الطاقة والمفاعلات النووية والمولدات وغيرها.

بينما تركز حروب الشبكات على إدراكات المجتمع Perceptions وأفكاره البنيوية وثوابته الاجتماعية، وعلى ثقة المجتمع في أفراده وصورته التي يرى بها نفسه.

ويمكن تنفيذ ذلك من خلال وسائل الدعاية والإعلان والعلاقات الدبلوماسية، والحروب النفسية، ومحاولة التخريب السياسي والثقافي، عبر تضليل وسائل الإعلام المحلية، ومحاولة تدعيم الحركات السياسية المعارضة عبر شبكات الكمبيوتر والإنترنت ومواقع التواصل الاجتماعي.

وفيما يلي نطرح أبرز خصائص وسمات حروب مواقع التواصل الاجتماعي:

أولاً: الأسئلة الرئيسية حول حروب مواقع التواصل الاجتماعي تعتبر حروب مواقع التواصل الاجتماعي، أحد الظواهر الحديثة المرتبطة بتزايد دور مواقع التواصل في التأثير على الأحداث السياسية والتفاعلات اليومية، ليس فقط على المستوى الاجتماعي، بل وأيضاً على المستوى السياسي والأمني، ولمّا كانت هذه الظاهرة حديثة، فإنها تطرح عدداً من الأسئلة الرئيسية الخاصة عن ماهية هذه الحروب والعناصر المشتركة فيها وكيفية إدارتها وهل يمكن تحقيق الانتصار فيها؟، وفيما يلي محاولة للإجابة عن هذه الأسئلة:

1- ما هي حروب مواقع التواصل الاجتماعي؟

لا يوجد تعريف محدد لحروب مواقع التواصل الاجتماعي؛ نظراً لحداثتها، وعدم وضوح أو اكتمال أبعادها. فهي ظاهرة مازالت تتشكل، ويمكن النظر إليها على أنها "استخدام الشبكات الاجتماعية لجذب اهتمام الرأي العام، سواء المحلي أو الإقليمي أو الدولي، أو محاولة التأثير عليه أو توجيهه أو تضليله، عبر وسائل التواصل الحديثة، سواء كانت مواقع إنترنت أو تطبيقات هاتفية للتواصل الاجتماعي، خلال فترة زمنية معينة، مدفوعاً بعوامل سياسية أو عسكرية". ومن أبرز الأمثلة على ذلك، الحرب على مواقع التواصل الاجتماعي بين حماس وإسرائيل خلال العدوان المتكرر على غزة، وحروب الهاشتاجات Hashtags بين الحركات السياسية وبعضها البعض، حيث يسعى كل طرف منهم دائماً إلى إبراز اعتداءات الطرف الآخر عليه، ومحاولة الظهور أمام الرأي العام الإلكتروني المتشكل على مواقع التواصل الاجتماعي باعتباره ضحية تدافع عن نفسها، كما أنها ليست بحرب معلومات؛ فالمعلومات رغم أهميتها في هذه الحرب إلا أنها ليست هدفاً لطرفيها، بل وسيلة يتم استخدامها لجذب أهدافها المتمثلة في مستخدمي مواقع التواصل الاجتماعي الذين يشكلون رأياً عاماً إلكترونياً قادراً على التأثير في الرأي العام المحلي والدولي.

وتظهر هذه الحرب أيضاً على مستويات أقل من التدخل العسكري، فالتطورات السياسية سواء كانت داخلية أو إقليمية، تجد - وبصورة فورية - طريقاً لها عبر مواقع التواصل الاجتماعي؛ مثل الانتخابات والاستفتاءات والاستطلاعات والقوانين وغيرها من الأحداث التي لا يتوفر حولها إجماع؛ حيث تبدأ الهاشتاجات Hashtags في الانتشار، ما بين مؤيد ومعارض، ويحاول كل طرف أن يبرر وجهة نظره ويستقطب الطرف الآخر لها.

وفي ذلك فهي تختلف عن الحروب السيبرية Cyberwars التي يُنظر إليها باعتبارها "القدرة على الدفاع عن والهجوم على المعلومات، من خلال شبكات الحاسب الآلي عبر الفضاء الإلكتروني، بالإضافة إلى شلّ قدرة الخصم على القيام بنفس هذه الهجمات"، وفي ذلك يرى "كينث جريس" أن الحرب السيبرية تشمل خمسة عناصر رئيسية هي: التجسس، الدعاية، الحرمان من خدمة الإنترنت، تعديل البيانات والتلاعب بها، والتلاعب أيضاً بالبنية التحتية[32].

2- ما هي الخصائص المميزة لهذا النوع من الحروب؟

لحروب مواقع التواصل الاجتماعي سمات رئيسية؛ فساحة القتال فيها افتراضية، ولا توجد بها حدود جغرافية أو إقليمية يمكن احتلالها أو طرد عدو منها، والحرب فيها دون رصاص أو حطام، والخسائر ليست بها أشلاء أو ركام، كما أن الأسلحة المستخدمة ليست لديها قدرة على تدمير العدو أو إزالته. وتلعب التكنولوجيا دوراً هاماً في هذه الحرب؛ فالطرف الذي يمتلك البرامج المتطورة والقادرة على تحليل مواقع التواصل الاجتماعي، وتحقيق التفاعل بين المستخدمين عبرها، واختيار أفضل الأوقات لبث الأفكار والحجج التي تؤيد رأيه، هو الذي تكون له الغلبة في النهاية، ولعل أبرز سمات هذه الحروب أنها[33]:

- مرتبطة بالتطورات السياسية والعسكرية على أرض الواقع.

- يشارك فيها المدنيون بصورة أكثر من العسكريين.

- ليست بها هدنة، حتى لو تحققت على أرض الواقع، ولا يمكن إيقافها.

- عدم القدرة على السيطرة على المشاركين فيها، لأنها تعبر عن عقيدة شخصية.

- لا يمكن فيها تدمير العدو كلياً أو إزالته.

3- من الذي يدير الحرب؟

يشارك في حروب مواقع التواصل الاجتماعي العديد من الفواعل، تبدأ بالأفراد، وتنتهي بالدول، مروراً بالحركات الإرهابية والأحزاب السياسية وجماعات الضغط والمصالح والناشطين السياسيين، ويشترك في إدارة هذا النوع من الحروب العديد من الجهات منها:

- الدول والأجهزة السيادية، بما تمتلكه من برامج مراقبة وتحليل للمواد المنشورة على مواقع التواصل الاجتماعي، ومتابعة الحسابات الشخصية النشطة، أو خلق حسابات وهمية أو إنشاء كتائب إلكترونية لبث أفكار معينة، وخلق اتجاه رأي عام إلكتروني على مواقع التواصل، حتى وإن كان غير حقيقي.

- الشركات التي تمتلك مواقع التواصل الاجتماعي، بما تمتلكه من قدرة على إدارة الحسابات الشخصية أو غلق بعض الحسابات أو الصفحات أو تغيير معدلات ظهورها في نتائج البحث الخاص بها، أو عقد اتفاقات مع بعض الدول لتسهيل حصولها على معلومات حول المستخدمين.

- قادة الرأي العام، بما لديهم من مصداقية لدى الرأي العام، وكذلك بعدد المشاركين والمتابعين لهم على هذه المواقع، الذين قد يصلون إلى الآلاف وفي بعض الأحيان إلى الملايين؛ والذين يساهمون في نشر أفكارهم وآرائهم حول القضايا المثارة.

- المستخدمون التقليديون، بما لديهم من قدرة على ترجيح كفة أحد الأطراف، من خلال المشاركات التي يتبنوها، ومن خلال قدرتهم على خلق اتجاه عام حقيقي داخل مواقع التواصل الاجتماعي.

4- ما هي معايير الانتصار؟

لا يوجد في حروب مواقع التواصل الاجتماعي منتصر ومهزوم، فالانتصار نسبي لكل منهما، فالطرف الذي يمتلك التكنولوجيا وقادر على تسويق حججه وأفكاره، يتفوق على الطرف الأخر ولكن دون أن يستطيع إخراجه من هذه الحرب. ولمعرفة إلى أي مدى استطاع أحد طرفي الحرب أن يحقق انتصاراً نسبياً على الآخر، يمكن الرجوع إلى عدة معايير، منها معايير كمية وأخرى معايير كيفية تتمثل في التالي:

- المعايير الكمية: وفيها يتم الاعتماد على عدد المؤيدين للطرف المنتصر سواء بمشاركة أفكاره أو أخباره أو الدفاع عن موقفه عبر مواقع التواصل الاجتماعي، وفيها يمكن الاستناد إلى معدل المشاركات Content Sharing على مدار اليوم، وعدد المشتركين Subscribers والمعجبين Like والمتابعين Followers، والاتجاه السائد على مواقع التواصل Website Trendin.

- المعايير الكيفية: والتي تتمثل في نوعية المشاركين في هذه الحرب، أو الوزن النسبي لهم داخل المجتمع؛ فكلما كان المشاركون من قادة الرأي العام والمؤثرين فيه محلياً وإقليمياً ودولياً، مثل الرموز السياسية والفنانين وموظفي المنظمات الدولية، كان الطرف أقرب للانتصار، وليس مجرد الاكتفاء بمشاركة المستخدمين التقليديين.

ثانياً: ما هي الأدوات المستخدمة في حروب التواصل الاجتماعي؟

للأدوات التي يتم استخدامها في هذا النوع من الحروب سمة خاصة، تُلائم طبيعة مواقع التواصل الاجتماعي؛ فنجد أن بعضها يوجد داخل مواقع التواصل، مثل المعلومات والصور والفيديوهات والهاشتاجات، وبعضها خارج هذه المواقع مثل برامج الكمبيوتر العملاقة التي تعمل على تحليل البيانات ومراقبة النشاطات على مواقع التواصل، وبعضها حقيقي وليس افتراضياً مثل الكتائب والجيوش الإلكترونية، وفيما يلي أبرز هذه الأدوات:

1 - المعلومة: وهي أهم أداة في هذا النوع من الحروب، سواء من خلال توفير المعلومات الصحيحة للمشاركين في هذه الحرب، أو الرد على المعلومات المغلوطة والإشاعات التي يتم تداولها.

2 - الصورة والفيديو: حيث تعتبر المؤثرات البصرية متمثلةً في الصور والفيديو أكثر الأدوات تأثيراً وقدرة على الإقناع وجذب مشاركين.

3 - السبق بالنشر: غالباً ما تحظى الموضوعات التي يتم نشرها أولاً بأكبر قدر من المشاركات، سواء كانت صحيحة أم خاطئة، لذلك فإن الطرف الذي يسبق بنشر فكرة أو معلومة، غالباً ما يجد صدىً لدى مستخدمي مواقع التواصل الاجتماعي بصورة أكبر من الطرف اللاحق.

4 - الكتائب الإلكترونية: وهي عبارة عن مجموعة من الأشخاص المنظمين والمدربين على استخدام التكنولوجيا الحديثة ووسائل الاتصال، يتميزون بكثافة نشاطهم وتواجدهم على مواقع التواصل الاجتماعي، ويتم إمدادهم بالمعلومات بهدف نشرها عبر متابعيهم ومستخدمي هذه المواقع، وتكون مهمتهم الرئيسية هي الدفاع عن مصالح الدولة ومواقفها تجاه الأحداث.

5 - برامج إدارة حروب التواصل الاجتماعي: وهي تلك البرامج التي تعمل على تحليل البيانات والمعلومات المتاحة على مواقع التواصل الاجتماعي، كما أنها تستطيع أن تؤثر على الاتجاهات Trends السائدة عليها وتغير من نتائج ظهورها على محركات البحث الخاصة بها، ليس هذا وحسب، بل يمكنها مراقبة كافة أنشطة المستخدمين على مواقع التواصل في زمنها الحقيقي Real Time والتجسس على تحركاتهم الافتراضية ومكالمتهم الهاتفية عبر الإنترنت.

6 - الهاشتاج: وتقوم هذه الأداة بتصنيف الموضوعات المثارة عبر مواقع التواصل الاجتماعي، وتسهيل عملية الوصول إليها، وقد اكتسبت شهرة واسعة خلال الفترة الماضية لما لها من قدرة على الوصول إلى أكبر عدد من المستخدمين.

وفي هذا الإطار فإن أهم الأدوات المؤثرة في حروب التواصل الاجتماعي هما أداتي برامج الكمبيوتر والهاشتاج، ومن ثم فسيتم التركيز عليهما بصورة أكبر في هذه الدراسة:

- برامج إدارة حروب مواقع التواصل الاجتماعي:

تُدار حروب التواصل الاجتماعي من خلال برامج عملاقة تتكون من العديد من برامج الكمبيوتر، بالإضافة إلى وحدات التحليل البحثية التي تعمل على رصد ومتابعة ما ينشر في مواقع التواصل من ناحية، والرد على ما يثار في داخلها من ناحية أخرى. وقد كشفت تسريبات "إدوارد سنودن" الموظف السابق بوكالة الاستخبارات الأمريكية CIA ووكالة الأمن القومي الأمريكية NSA عن العديد من البرامج التي صممتها الإدارة الأمريكية واستخدمتها في حروب التواصل الاجتماعي، والتي كان منها:

Wind Stellar:-

وهو أحد برامج التجسس الإلكترونية الرئيسية التي ظهرت بعد أحداث الحادي عشر من سبتمبر مباشرةً، وكان الغرض منه هو التجسس المحلي على المقيمين داخل الأراضي الأمريكية. ويعمل البرنامج على التجسس على الاتصالات الهاتفية والمراسلات الإلكترونية[34] ، وقد استمر هذا البرنامج لمدة عامين في ظل إدارة الرئيس "أوباما" الأولى قبل أن ينهي عمله ويتم استبداله ببرامج أخرى.

EvilOlive - هو البرنامج الرئيسي الذي حلَّ محل برنامج Wind Stellar، وذلك في عام 2011، وكان الهدف الرئيسي منه هو جمع كميات كبيرة من المعلومات العملاقة الموجودة على الإنترنت، سواء كانت اتصالات أو معلومات تخص أفراداً داخل أو خارج الولايات المتحدة؛ حيث يستطيع هذا البرنامج أن يجمع نصف البيانات الحيّة التي يتم تراسلها عبر الإنترنت، وهو ما يعتبر نقلة نوعية في القدرات الكمية لبرامج التجسس، من حيث القدرة على جمع أكبر قدر من المعلومات[35].

ShellTrumpet- وقد تم الإعلان عن هذا البرنامج عام 2012، ويعمل على جمع بيانات عملاقة عبر الإنترنت من مختلف المستخدمين، ويفوق هذا البرنامج في قدراته برنامج EvilOlive، حيث تم الإعلان في ديسمبر 2012 أن هذا البرنامج جمع ترليونات من البيانات العملاقة، نصفها فقط تم في عام 2012[36] .

PRISM-:

وهو أحد البرامج التي تم تصميمها في إطار مكافحة الإرهاب. ويعمل برنامج "بريزم" على جمع معلومات من أشخاص، سواء داخل أو خارج الولايات المتحدة.

وبموجب قانون حماية أمريكا، يحق لوكالة الأمن القومي الأمريكي NSA أن تطلب من الشركات العاملة في مجال الإنترنت مثل "ياهو" و"فيس بوك" و"جوجل" و"أبل" و"مايكروسوفت" وغيرها، بيانات تتعلق بمستخدمين لها حول العالم[37] وهو ما سيتم توضيحه لاحقاً.

وقد قام "إدوارد سنودن" بتسريب معلومات لصحيفة "الجارديان" البريطانية حول برنامج "بريزم" في يونيه 2013؛ موضحاً أنه برنامج تجسس رقمي أمريكي مصنف بأنه سري للغاية يُشّغل من قبل وكالة الأمن القومي الأمريكية (NSA) بدأ منذ عام 2007، يتيح مراقبة الاتصالات الحيّة والمعلومات المخزنة، ويستهدف أي عميل لأي شركة منخرطة في البرنامج مثل شركة "جوجل" و"فيس بوك" و"تويتر" وغيرها، حيث يستطيع هذا البرنامج الحصول على معلومات تتضمن، رسائل البريد الإلكتروني، ومحادثات الفيديو والصوت، والصور، والاتصالات الصوتية ببرتوكول الإنترنت، وعمليات نقل الملفات، وإخطارات الولوج وتفاصيل الشبكات الاجتماعية[38].

- استراتيجية التواصل الفعّال عبر مواقع التواصل الاجتماعي "SMISC" أعلنت وكالة مشاريع البحوث الدفاعية المتطورة (DARPA) عام 2011 عن برنامج لاستخدام مواقع التواصل الاجتماعي في تحقيق التواصل الاستراتيجي Social Media in Strategic Communication program (SMISC)؛ حيث يهدف هذا البرنامج إلى تحقيق هدفين رئيسيين، الأول هو تحسين فهم وزارة الدفاع لما يجري على مواقع التواصل الاجتماعي في الوقت الحقيقي له Real Time وبخاصة في المناطق التي تنتشر فيها قوات أمريكية، أما الهدف الثاني، فهو قيام وزارة الدفاع باستخدام مواقع التواصل في بث رسائل إعلامية تخدم مصالحها الاستراتيجية [39].

- برامج الهويات المزيفة "Sock Puppet" وهي عبارة عن هويات غير حقيقية، يتم تدشينها من خلال برنامج إلكتروني على مواقع التواصل الاجتماعي بلغات مختلفة، بهدف بث رسائل تدعم

رؤية ما خلال فترة الأزمات، حيث يقوم أحد الأشخاص بالتحكم في عدد من الحسابات الشخصية الغير حقيقية على مواقع التواصل الاجتماعي في مناطق مختلفة من العالم، وهو ما يُمكّن الدولة من خلق اتجاه عام مزور نحو قضايا معينة في مواقع التواصل الاجتماعي، يمكن أن يؤثر في الأحداث السياسية[40]. - استراتيجية تحليل شبكات التواصل "SOCMINT" استخدمت الحكومة البريطانية استراتيجية (SOCMINT) Social Media Intelligence بهدف تحليل البيانات الموجودة على مواقع التواصل الاجتماعي والخروج بمؤشرات إحصائية حول المستخدمين النشطين والمؤثرين على مواقع التواصل الاجتماعي، وكذلك مؤشرات معلوماتية خاصة بعمليات الحشد والتعبئة التي تقوم بها بعض الحركات الجهادية على مواقع التواصل الاجتماعية.

- برامج اختراق الأجهزة الشخصية عبر التطبيقات الاجتماعية:

لما كان الاعتماد على الأجهزة المحمولة يتزايد؛ مثل الهاتف المحمول والحاسب اللوحي وغيرها، فقد أصبحت هدفاً للدول، بما يمكن أن توفره من معلومات حول مستخدميها؛ حيث يمكن اختراق بعض تطبيقات الهاتف المحمول وسرقة المعلومات الموجودة عليه، ومعرفة كافة البيانات المُخزنة في حساباته، مثل العمر والجنس والميول ومكان التواجد والمُستوى العلمي وغيرها.

حيث كشف تقرير نشرته صحيفة "الجارديان" البريطانية، أن وكالة الأمن القومي الأمريكية تقوم بتطوير تقنيات تسمح لها باستغلال تطبيقات الهواتف الذكية للوصول إلى معلومات خاصة بالمُستخدمين. كما سرب "إدورد سنودن" وثائق تؤكد استهداف وكالة الاستخبارات الأمريكية CIA بيانات الهاتف المحمول للمُستخدم وذلك لجلب معلومات عن الإرهابيين وأهداف استخباراتية أُخرى؛ حيث أنفقت ما يزيد على مليار دولار لصالح برامج التجسس الخاصة باستهداف الهواتف الذكية، ولتوضيح قُدرة برامج الوكالة؛ أشار التقرير إلى أنه وبمجرد قيام المُستخدم برفع صورة إلى وسائل التواصل الاجتماعي باستخدام هاتفه الذكي، تستطيع الوكالة جمع معلومات؛ مثل جهات الاتصال في هاتف المُستخدم، وعناوين البريد الإلكتروني، وموقع المُستخدم[41].

برزت مواقع التواصل الاجتماعي بشدة خلال فترة الثورات العربية؛ مما دفع بعض النظم السياسية إلى إغلاق هذه المواقع في بعض الأحيان، وسعت إلى إبرام مناقصات لشراء برامج عملاقة لمراقبتها وتحليلها ورصد تحركات الناشطين عليها. وقد كان لثورات الربيع العربي أثر هام في توجه كثير من دول المنطقة نحو هذه المواقع، سواء تلك التي أصابتها هبّات الربيع العربي أو التي لم تصبها، واتجهت إلى تشديد المراقبة عليها، وقام بعضها بشراء برامج كمبيوتر تعمل على مراقبتها وتحليل ما بها من مضمون.

ومن أمثلة ذلك ما حدث في أعقاب 25 يناير 2011؛ حيث عثر بعض الناشطين على وثائق خاصة بعزم الحكومة المصرية على التعاقد مع شركة Gamma International UK Limited للحصول على نسخة من برنامج FinSpy الذي تبلغ قيمته 287,000 يورو؛ وهو أحد برامج مراقبة الاتصالات عبر الإنترنت، بدايةً من برامج الدردشة الفورية وحتى مواقع التواصل الاجتماعي. وفي نفس الفترة أمدت شركة Amesys الفرنسية "معمر القذافي"، بناءً على طلبه، بحزمة من البرامج الفنية تدعى Eagles لكي تمكنه من مراقبة الإنترنت في ليبيا، سواء كان ذلك محادثات هاتفية أو برامج مراسلات فورية أو غيرها من مواقع التواصل الاجتماعي، بالإضافة إلى برامج لمنع الليبيين من استخدام البروكسي Proxy للدخول على المواقع المحجوبة في ليبيا[42].

أولاً: حالة شبكات التواصل الاجتماعي في منطقة الشرق الأوسط وفقاً لإحصاءات مؤسسة "We Are Social"، نلاحظ أن منطقة أمريكا الشمالية تأتي في المرتبة الأولى من نسبة مستخدمي الشبكات الاجتماعية في العالم بنسبة 56% يليها أوروبا الغربية بنسبة 44%، بينما تحتل منطقة الشرق الأوسط المركز التاسع بنسبة 24% وفقاً للتقرير الصادر حتى يناير 2014.

وقد أصدرت قمة رواد التواصل الاجتماعي المنعقدة في دبي، تقريراً عام 2015 عن حالة استخدام مواقع وتطبيقات التواصل الاجتماعي في الدول العربية خلال عام 2015، وقد أظهرت بعض النتائج أن موقع ال"فيس بوك" وتطبيق ال"واتس آب" هما أكثر المنصات الاجتماعية استخداماً بين سكان منطقة الشرق الأوسط؛ حيث يأتي استخدام ال"فيس بوك" بنسبة 87%، يليه تطبيق ال"واتس آب" بنسبة 84%، ثم موقع ال"يوتيوب" بنسبة 39%، يليهم تطبيق ال"إنستجرام" بنسبة 34%، ثم "تويتر" بنسبة 32% وهو ما يوضحه الشكل التالي:

حيث كان موقع ال"فيس بوك" هو الأكثر استخداماً في 10 دول عربية وفقاً للتقرير هي (الإمارات العربية المتحدة وقطر وعمان والأردن وفلسطين والعراق واليمن وليبيا ومصر والمغرب). ومن جهة أخرى، فقد كان "واتس آب" وسيلة التواصل الاجتماعي الأكثر استخداماً في كل من (السعودية والكويت والبحرين وسوريا ولبنان والسودان والجزائر ومصر والمغرب)[43].

كما يوضح الشكل التالي نسب استخدام موقع ال"فيس بوك" كمنصة اجتماعية للتواصل في كل دولة على حدة، وفقاً لتقرير قمة رواد التواصل الاجتماعي العرب.

بينما يوضح الشكل التالي نسب استخدام تطبيق ال"واتس آب" في كل دولة عربية على حدة:

ويوضح الشكل التالي نسب استخدام موقع "تويتر" كمنصة اجتماعية في منطقة الشرق الأوسط.

أما فيما يتعلق بتطبيق ال"إنستجرام" فيوضح الشكل التالي أكثر الدول استخداماً له في منطقة الشرق الأوسط.

أما نسبة مشتركي موقع ال"يوتيوب" فيوضحها الشكل التالي:

أما النسبة المئوية لإجمالي مستخدمي موقع "جوجل بلس" فهي:

وبالنظر إلى الإحصاءات التي يقدمها موقع App Annie المتخصص في تحليل أسواق تطبيقات الهواتف الذكية؛ نجد أن في مصر، 9 تطبيقات من بين أول 15 تطبيقاً في عدد مرات التحميل هي للتواصل الاجتماعي وذلك على الهاتف iPhone الذي يعمل بنظام تشغيل IOS، أما الهواتف التي تعمل بنظام تشغيل "أندرويد" فنجد أن من بين أول 15 تطبيقاً، 7 تطبيقات منها هي تطبيقات للتواصل الاجتماعي.

وفي الكويت نجد أن 9 تطبيقات هي للتواصل الاجتماعي من بين أعلى 15 تطبيقاً تم تحميلهم على برنامج "أندرويد"، في حين بلغت عدد التطبيقات الاجتماعية على برنامج IOS للتواصل الاجتماعي 8 تطبيقات من بين أعلى 15 تطبيقاً.

وفي لبنان نجد أن من بين أكثر التطبيقات تحميلاً، 8 تطبيقات منها للتواصل الاجتماعي تم تحميلها على برنامج IOS، بينما بلغت التطبيقات الاجتماعية الأكثر تحميلاً على ال"أندرويد" 6 تطبيقات.

وفي البحرين من أبرز 15 تطبيقاً يأتي 11 تطبيقاً على IOS للتواصل الاجتماعي، و9 تطبيقات للتواصل الاجتماعي على نظام تشغيل ال"أندوريد".

وفي الأردن من أبرز 15 تطبيقاً، 8 تطبيقات منها للتواصل الاجتماعي على برنامج IOS، و7 منها على برنامج تشغيل "أندرويد".

وفي قطر 9 تطبيقات للتواصل الاجتماعي على برنامج IOS و7 على برنامج ال"أندرويد".

وفي السعودية 5 تطبيقات للتواصل الاجتماعي على IOS و10 تطبيقات على ال"أندرويد".

ثانياً: معضلة مواقع التواصل الاجتماعي في مصر شهدت مصر خلال ثورة 25 يناير وما بعدها العديد من التفاعلات على الشبكات الاجتماعية، الأمر الذي دفع أجهزة الأمن المصرية إلى إغلاقها بشكل نهائي أثناء المظاهرات التي اندلعت اعتباراً من مساء الخميس الموافق 27 يناير 2011، واستمر القطع حتى أعيدت الخدمة ظهر الأربعاء الموافق 2 فبراير 2011[44] ، وأصيبت خدمة الإنترنت في مصر بالشلل التام، وفشل جميع المستخدمين في الوصول إلى مواقع التواصل الاجتماعي، سواء من خلال الهواتف المحمولة، أو أجهزة الكمبيوتر. وقد رأت وزارة الداخلية أن في التفاعلات والمشاركات التي تجري عبر الشبكات الاجتماعية ما يهدد السلم والأمن العام، وهو ما دفعها لشراء أنظمة مراقبة لهذه الشبكات، حيث قامت صحيفة "الوطن" في شهر يونيو 2014 بعمل انفراد صحفي أتبعه العديد من التصريحات الرسمية وذلك من خلال نشرها لكراسة الشروط والمواصفات التي وضعتها وزارة الداخلية لمشروع رصد المخاطر الأمنية لشبكات

التواصل الاجتماعي (منظومة قياس الرأي العام) من أجل تطوير وتوريد وتركيب رخص برامج وتطبيقات وأجهزة المشروع الذي يهدف لإحكام قبضتها الأمنية على مواقع التواصل الاجتماعي، عن طريق البحث عن المصطلحات والمفردات المختلفة التي تكون مخالفة للقانون والآداب العامة، وتقديم أداة تحليلية للآراء والاتجاهات المعروضة وأهدافها، ودعم اتخاذ قرار بشأنها.

ويرتبط نظام المراقبة ببعض المواقع والتطبيقات، مثل "فيس بوك"، "تويتر"، "يوتيوب"، "واتس آب"، "إنستجرام، "فايبر" و"لينكيد إن"، على أن تكون المراقبة داخل وزارة الداخلية من خلال أجهزة الخدمات الرئيسية. ويتمتع النظام بقدر من المرونة تتيح له التغير والتوافق مع المتطلبات الأمنية الجديدة، كما يتيح هذا البرنامج، إمكانية مشاهدة كل ما يُكتب على مواقع التواصل الاجتماعي بطريقة التسلسل الزمني، بشكل فوري وسريع دون الحاجة لانتظار فترات طويلة، حيث تظهر آلاف المشاركات من المستخدمين بصورة آلية، ويتعامل البرنامج مع متصفحات إنترنت "إكسبلورر"، "فاير فوكس" و"جوجل كروم"، ويمكّن مديره من معرفة الشخصيات المؤثرة في كل منطقة، لكن البرنامج لا يتيح مشاهدة رسائل "فيس بوك" أو "تويتر"[45].

وهو ما أثار عاصفة من الانتقادات ضد وزارة الداخلية خاصة أن الدستور المصري ينص في المادة 57 من على أن "للحياة الخاصة حرمة، وهي مصونة لا تمس.

وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك"[46].

وقد أعقب ذلك العديد من المناقشات في وسائل الإعلام المختلفة، وتقدمت بعض من منظمات المجتمع الحقوقية بالدعوى رقم 63055 لسنة 68 قضائية، للمطالبة بوقف تنفيذ وإلغاء قرار وزارة الداخلية بإجراء ممارسة محدودة، تستهدف شراء تطبيقات تمكّنها من مراقبة الشبكات الاجتماعية على الإنترنت[47] ، إلا أن الأمر انتهى بتعاقد وزارة الداخلية مع شركة مصر للنظم الهندسية "see Egypt"، التابعة لشركة "blue coat" المتخصصة في مراقبة أنشطة الإنترنت، وقد زودت السلطات المسؤولة بأجهزة مراقبة حديثة تزيد من كفاءة مراقبة مواقع الإنترنت، وتعمل على اختراق العديد من المواقع مثل "فيس بوك، تويتر، يوتيوب وسكايب"[48] ، ليتمكن رجال مباحث الإنترنت من كشف أي عمليات إرهابية أو أخبار أو فيديوهات تتنافى مع قيم المجتمع.

ولكن يتبقى هنا سؤال جوهري، خاصةً بسبب قيام الأفراد بنشر معلومات شخصية على الشبكات الاجتماعية رغم معرفتهم أنها مراقبة، ويمكن توضيح ذلك في أن كثيراً من الأفراد يعتقد أنه يستطيع التحكم في خصوصيته من خلال إعدادات الخصوصية Privacy setting في الشبكات الاجتماعية، غافلاً أو متغافلاً عن التكنولوجيات الذكية التي يمكنها مراقبة كل شيء بما

فيها رسائله الشخصية، كما أن الطريقة التي يتم تصميم مواقع التواصل الاجتماعي بها تتطلب من الأفراد إفشاء الكثير من معلوماتهم الشخصية، مثل مكان الميلاد والدراسة والسكن والعمل والحالة الاجتماعية والتوجهات السياسية والكتب المفضلة والأفلام المشاهدة والموسيقى المحببة وغيرها من البيانات الشخصية الدقيقة عن حياة المستخدم، وهو يستجيب لكل هذه الأسئلة رغبة منه في الحصول على الخدمات المجانية التي تقدمها هذه المواقع ورغبة في اقتحام تفاصيل هذا العالم الافتراضي، لذا سيتمر الأفراد في إفشاء المزيد من بياناتهم الشخصية طواعية على الشبكات الاجتماعية، رغم علمهم بالمخاطر التي قد يتعرضون لها.

ثالثاً: أبرز ملامح حروب التواصل الاجتماعي على المستوى الداخلي للدول تميزت حروب مواقع التواصل الاجتماعي في دول منطقة الشرق الأوسط بعدة سمات، غلب عليها الطابع الأمني؛ منها استخدام هذه المواقع في تنظيم المظاهرات والاحتجاجات، سواء كانت واقعية أو افتراضية، أو تشكيل جبهات حرب افتراضية بين أنصار ومعارضي أحد التيارات السياسية أو الفكرية، سواء كان محلياً أو إقليمياً، ويتضح ذلك في التالي[49]:

1- "إثارة" أو "إعادة توجيه" الرأي العام يتم استخدام الشبكات الاجتماعية كأحد الوسائل الأساسية للتضليل الإعلامي وبث المواد التحريضية والداعية لشق الصف بين فئات المجتمع المختلفة، وكذلك لنشر الشائعات التي تهدف دائماً لخلق حالة لا نهائية من عدم الاستقرار، سواء بنشر مقالات أو أخبار كاذبة أو استخدام صور غير حقيقية معدلة ببرامج مثل برنامج ال"فوتوشوب". بل يذهب المضللون أحياناً لاستخدام صور حقيقية لا تخص القضية المثُارة أساساً بغرض الترويج لأحداث عنف أو فتنة طائفية.

وهناك عدد كبير من الأمثلة التي احتوت صوراً أو لقطات فيديو لمشاهد مصابين أو جرحى في مصر أثناء فترة ثورة 25 يناير وبالبحث عن مصادرها يثبت أنها لجرحى في تفجير ببغداد أو سوريا على سبيل المثال، أو أحياناً تستخدم صور حقيقية من مصر في غير سياقها بغرض إقناع مستخدمي الإنترنت بمعلومات زائفة.

فمثلاً تم تداول صورة نشرتها إحدى المواقع الإلكترونية أثناء أحداث ماسبيرو في مصر في أكتوبر 2011، على أنها صورة لجثث وقعت أثناء الأحداث، وبالتدقيق وجد أن الصورة تعود لانتشال بعض الجثث أثناء أحد السيول في جدة[50].

ويساعد على ذلك، سهولة نشر الشائعات وسرعة نقلها بين المستخدمين، وهنا يصعب على المستخدم التفرقة بين المعلومة والشائعة، كما يصعب التأكد من صدق المعلومة، ويصعب التحقق من كذب الشائعة، ومن ثم تنتشر معلومات خاطئة بين الأفراد، قد تتناول شخصيات سياسية أو رموز مجتمعية أو قضايا سياسية، أو معلومات اقتصادية يترتب عليها خسائر مالية، وفي نفس الوقت يصعب تحجيم نطاق هذه الشائعات، وفي حالة نفيها أو الرغبة في تصحيحها، فإن المعلومة الصحيحة لا تجد نفس مستوى الانتشار الذي بدأت به الشائعة.

وقد تعددت في مصر الشائعات التي تم تداولها عبر هذه المواقع خلال عام 2014، والتي كان أبرزها خبر وفاة الرئيس الأسبق "حسني مبارك"، وشائعة معاقبة أي طالب أو مدرس بغرامة 30

ألف جنيه أو الحبس لمدة عام في حال التحرك أثناء تحية العلم، وقد نفت وزارة التربية والتعليم هذه الشائعة جملة وتفصيلاً. وكذلك انتشار شائعة انهيار أجزاء كبيرة من هرم "زوسر" المدرج بسقارة، وشائعة طرح لوحة معدنية تحمل اسم الرئيس عبد الفتاح السيسي "السيسي1" سيتم تقدير ثمنها بنحو 30 مليون جنيه في مزاد علني لبيع اللوحات المعدنية لدعم صندوق "تحيا مصر"، كل هذه الإشاعات وغيرها وجدت طريقاً لها عبر مواقع التواصل الاجتماعي[51].

إلى جانب ذلك، يلاحظ تزايد دور الكتائب الإلكترونية في تشويه منظم للرموز السياسية سواء كانت شخصيات أو دول أو مؤسسات من خلال الإنترنت، خاصة بعد الاستخدام الفعّال لخاصية "الهاشتاج" في موقع "تويتر"؛ حيث يتم استخدامه من قبل التيارات السياسية في معاركها الانتخابية[52]. على سبيل المثال، استخدم بعض شباب الإخوان المسلمين والمعارضين لترشح الرئيس "عبدالفتاح السيسي" في الانتخابات الرئاسية 2014، هاشتاجاً مسيئاً وتم الرد عليه بهاشتاج آخر يحاول أن يفضح جرائم الإخوان في العالم باسم (#mb_europe).

كما تم التهكم على وزارة الداخلية المصرية حينما صرحت بمراقبة مواقع التواصل الاجتماعي، من خلال هاشتاج "#إحنا_متراقبين". كما تعددت الهاشتاجات التي تسخر من قطر بسبب موقفها الداعم للإخوان المسلمين. وقبل انعقاد مؤتمر دعم الاقتصاد المصري، وعلى خلفية الإساءات المتكررة التي توجهها قناة الجزيرة إلى مصر انطلق هاشتاج احتل المرتبة الأولى عالمياً يسخر من قطر، وهو ما توضح الصورة التالية.

2- التشويه السياسي الإلكتروني ويقصد به تشويه الرموز السياسية سواء كانت شخصيات أو دول أو مؤسسات من خلال الإنترنت، خاصة بعد الاستخدام الفعّال لخاصية "الهاشتاج" بموقع "تويتر"، حيث يتم استخدامه من قبل التيارات الفكرية في حروبهم السياسية ومعاركهم الانتخابية، وقد اتضح ذلك في:

- الإساءة للشخصيات: فتم استخدام هاشتاج مسئ من قبل بعض شباب الإخوان المسلمين والمعارضين لترشح الرئيس "عبد الفتاح السيسي" للانتخابات المصرية، وتم الرد عليه بهاشتاج مسئ يتناول الرئيس السابق وجماعته.

- الإساءة للدول: وظهر ذلك عند انتقاد دولة قطر والأسرة الحاكمة على مواقع التواصل الاجتماعي على خلفية موقفها الداعم للإخوان المسلمين، وموقفها من الثورة المصرية.

- الإساءة للمؤسسات: من خلال انتقاد وزارة الداخلية المصرية حينما صرحت بمراقبة مواقع التواصل الاجتماعي، فزخرت المواقع بالسخرية من القرار كرد فعل عكسي من الناشطين الإلكترونيين.

3- الاحتجاجات الإلكترونية ومن ظواهر الاحتجاج الإلكتروني قيام بعض الشباب في مصر عبر مواقع التواصل الاجتماعي بالاحتجاج على خدمات الإنترنت، وظهرت بعض الحملات الإلكترونية في زمن قصير نادت بالتصعيد ضد هذه الشركات، الأمر الذي دفعها إلى الاستجابة بصورة مباشرة إلى هذه المطالب بتخفيض أسعار الخدمة والعمل على تحسينها.

4- المظاهرات الافتراضية مثّلت مواقع التواصل الاجتماعي خلال فترة الثورات العربية الوقود المغذي لها، خاصةً في الدول كثيفة السكان مثل مصر، فساعدت على الحشد والتنظيم والانتقال من المجال الافتراضي إلى المجال الواقعي، فخرج آلاف وملايين المواطنين رافعين مطالب ثورية انتهت بانهيار نظم سياسية.

أما في الدول قليلة السكان، فإن خروج عدد كبير من المواطنين في مظاهرات، غير كافٍ لإسقاط نظام سياسي، ولكن تستطيع مواقع التواصل أن تتسبب في إزعاج شديد لهذه النظم عبر تنظيم مظاهرات افتراضية.

ومن أبرز الأمثلة على المظاهرات الافتراضية قيام عدد من الشباب القطري تحت مسمى "حركة أحرار قطر" بالدعوة عبر مواقع التواصل الاجتماعي لثورة شعبية، كما حاول بعض شباب الإخوان في الإمارات خلال فترة الثورات العربية، استخدام مواقع التواصل الاجتماعي للدعوة إلى وقفة احتجاجية في الإمارات تطالب بإجراء تعديلات على بنية النظام السياسي للدولة.

5- حرب افتراضية بين تيارات سياسية عادةً ما يتم استخدام مواقع التواصل الاجتماعي في دول المنطقة العربية للسجالات الفكرية بين التيارات السياسية والفكرية، وقد حدث هذا مراراً في أعقاب الانتخابات البرلمانية أو الرئاسية والاستفتاءات التي شهدتها عدة دول عربية ومنها مصر. فهناك دائما معارك افتراضية مشتعلة بين أنصار الرئيس "مبارك" ومعارضيه، ومعارك بين أنصار الإخوان ومعارضيهم، ومعارك بين مؤيدي ومعارضي النظام في سوريا، وهو الأمر نفسه الذي حدث في أعقاب الانتخابات الرئاسية الجزائرية، التي شهدت جدلاً بين مؤيدي ومعارضي الرئيس "عبد العزيز بو تفليقة"، بل إن الأمر انتقل لمستويات أقل من ذلك فشمل الجدال حول القوانين الداخلية والقرارات السياسية والتصريحات الرسمية، التي عادةً ما تلقى ردود فعل ساخرة أو مهاجمة لها.

6- الابتزاز الإلكتروني وهو من أكثر الجرائم الإلكترونية انتشاراً، من خلال قيام أحد القراصنة الهواة Amateur Hacker باختراق بريد أو حساب رسمي أو صحفة على مواقع التواصل الاجتماعي، بهدف بث رسائل سياسية على لسان الضحية، أو ابتزازها للحصول على المال، وغالباً ما يكون الضحية هو السبب في ذلك، من خلال التساهل في اتباع الإجراءات الأمنية، مما يسهل على القراصنة الحصول على المعلومات. وفي حالة استجابة الضحية لمطالب ال"هاكر" بدفع أموال مقابل عدم نشر بيانات أو صور شخصية للضحية خوفاً من الفضيحة ودون لجوء للسلطات المختصة، فإنه يقوم بابتزازه مرات أخرى.

7- التحرش الالكتروني يعد التحرش الإلكتروني واحداً من الممارسات السلبية الشائع استخدامها خاصةً على مواقع التواصل الاجتماعي؛ حيث يقوم المتحرش بالاتصال الإلكتروني مع الضحية بشكل متكرر وغير مرغوب فيه، كما يقوم بتتبع كافة أنشطة الضحية على الإنترنت بقصد الإزعاج وإحداث الضرر النفسي للضحية أو تهديدها، أو إذلالها أو الأخذ بالثأر منها.

ويعد الفارق الجوهري بينه وبين الابتزاز الإلكتروني هو حرص المتحرش على تعريف الضحية بما يقوم به من تتبع لأفعالها، حتى يرى ردود أفعال الضحية ويشعر بنجاحه في إزعاج ضحيته.

ويتم ذلك من خلال عدة أدوات منها نشر رسائل نصية وتعليقات على مواقع التواصل الاجتماعي، أو إرسال بريد الكتروني، أو نشر صور جرافيك للضحية على مواقع التواصل الاجتماعي أو على الموبايل.

وقد زاد زخم التفاعل الإلكتروني بشأن قضية التحرش بعد الواقعة الشهيرة التي تعرضت لها فتاة مصرية في ميدان التحرير أثناء احتفالات الشارع بتنصيب الرئيس الجديد. وظهرت العديد من الحملات الإلكترونية لتتبع المتحرشين سواء في العالم الافتراضي أو في الواقع من خلال نشر المعلومات المتاحة عن الشخص وصوره والفيديوهات التي تؤكد ما قام به من تحرش، أو من خلال تنظيم حملات إلكترونية لحث الشباب على الدفاع عن المرأة، وحملات أخرى لتوعية الفتيات بأساليب "الدفاع عن النفس" في حالة تعرضت للتحرش.

ويعتبر هاشتاج "هنتحرش بالرجالة" من أكثر الحملات تفاعلاً؛ حيث يطالب الفتيات باتباع ذات السلوك لإزعاج الشباب وإلحاق الأذى بهم، وعلى الرغم من طابع السخرية والتهكم في هذا الطرح، إلا أنه بشكل عام يلفت النظر إلى ظاهرة "الثأر الجماعي" حيث لا ينصبّ رد الفعل على القائم بالفعل فقط وإنما على كل من ينتمي لفئته أو نوعه.

8- الغش الإلكتروني بدأت هذه الظاهرة في الانتشار خلال السنوات الماضية، من خلال سماح بعض لجان الامتحانات باصطحاب الهواتف الذكية داخل اللجان؛ فيقوم عدد من الطلبة بوضع أسئلة الامتحان على صفحات التواصل الاجتماعي مما يساعد في عملية غش جماعي والإخلال بمبدأ تكافؤ الفرص.

وقد انتشرت هذه الظاهرة في مصر بوضوح، وتسببت في إعادة بعض الامتحانات خاصة للشهادة الثانوية عام 2014، ومن أشهر الهاشتاجات المصرية الخاصة بتسريب أسئلة الامتحانات "غشاشون _ فدائيون، وبردو _ هنغش، وثانوية _ عامة، والحارة _ المزنوقة، وعبيلوا _ واديلو"، فأصبح الهاشتاج أحد أخطر الأدوات التي تتم من خلالها عمليات الغش الإلكتروني الجماعي، مما دفع بعض الخبراء في مصر إلى المطالبة بإعلان وفاة نظام الثانوية العامة الذي يعتمد على أوراق الامتحانات التقليدية.

ولا تقتصر هذه الظاهرة على الدول النامية فقط، بل قامت إحدى المدارس في مدينة "نيويورك" العام الماضي بالغاء أحد الامتحانات بعد تسريبها على الإنترنت، كما قامت جامعة "كويوتو" اليابانية بتغيير أسئلة امتحانات الرياضيات واللغة الإنجليزية بعد تسريبها على شبكة "ياهو" عام 2011.

ورغم محاولات وزارات التعليم تشديد الإجراءات ومنع استخدام الهواتف المحمولة داخل اللجان، مازالت الظاهرة مستمرة، فالتطور الذي وصلت إليه أدوات الاتصال من صغر في الحجم وكفاءة في نقل البيانات، يتم توظيفها سلبياً في عمليات الغش داخل لجان الامتحانات.

حيث يمكن للطالب أن يتواصل مع طرف آخر من خلال سماعة صغيرة تعمل بخاصية ال"بلوتوث"، ومتصلة بهاتف محمول على مقربة من لجنة الامتحان. كما يمكن للفتيات المحجبات أن تستخدمن هاتفاً محمولاً صغيراً، أو جهاز MP 3حجمه عدة مليمترات في عملية

الغش دون أن يلاحظ أحد المراقبين ذلك، وتصبح مسألة تأمين أسئلة الامتحانات في غاية الأهمية خاصة إذا كانت وزارة التعليم تعتمد نظاماً إلكترونياً لحفظ وأرشفة هذه الامتحانات.

9- ازدهار التجارة غير الشرعية حيث تحولت هذه التطبيقات، إلى منصات يتم من خلالها الإتجار في الرقيق والمخدرات والأجهزة المحظورة بموجب القانون. ففيما يتعلق بتجارة الرقيق؛ تجد كثير من بائعات الهوى نافذة لهن عبر مواقع التواصل الاجتماعي لتقديم خدماتهن لمتصفحي هذه المواقع. وليس من الغريب أن نجد كثيراً منهن يضعن بيانات خاصة بهن وبالطريقة التي يمكن الوصول إليهن بها، ويغلب على بائعات الهوى استخدام طريقة "كروت الشحن" وهي كروت شحن الهاتف المحمول بفئاتها المختلفة؛ حيث تطلب الفتاة من ضحيتها إرسال كرت شحن بفئة معينة لرقم معين مقابل موعد غرامي على الإنترنت، أو إرسال مبلغ أكبر لتحديد مكان للمقابلة الحقيقية وليس الافتراضية، ورغم سهولة إيقاع الضحية في قبضة أجهزة الأمن، إلا أن هذه الظاهرة تشكل خطراً بالغاً وبخاصة على القُصّر، من خلال تسهيل عرض المحتوى الإباحي على الشبكات الاجتماعية.

وفيما يتعلق بتجارة المخدرات، كشف تقرير صادر عن المجلس العالمي لمكافحة المخدرات the international narcotics control board والذي يراقب تطبيق اتفاقيات الأمم المتحدة لمكافحة المخدرات، أن هناك مخدرات ووصفات طبية غير مشروعة يتم شراؤها عبر الإنترنت من خلال صيدليات غير شرعية[53] ، وأوضح "حامد قدسي"، رئيس المجلس العالمي لمكافحة المخدرات، "أن صيدليات الإنترنت غير الشرعية أصبحت تستخدم مواقع التواصل الاجتماعي في الترويج لمواقعها وهو الشيء الذي سيُعرّض جمهوراً كبيراً لمخاطر المنتجات الخطيرة"[54].

ولم يقتصر الأمر على هذا النوع من المخدرات والأدوية المغشوشة، بل انتقل أيضاً ليشمل "المخدرات الرقمية"؛ وهي نوع من أنواع الموسيقى التي يتم تحميلها من خلال مواقع الإنترنت ويتم تسويقها عبر مواقع التواصل الاجتماعي، والتي قد تتسبب في اختلال وظائف الدماغ البشري، وتتسبب في أمراض نفسية وعضوية لمريديها.

كما أصبحت هذه التطبيقات جاذبة للمتاجرين في الأجهزة الغير مصرح بها، مثل الكاميرات وأجهزة التجسس غير المصرح بها، والصواعق الكهربائية وغيرها من الآلات الحادة أو الأسلحة النارية، خاصة موقع ال"فيس بوك"، حيث يقومون بانشاء صفحات خاصة بهم لعرض بضائعهم وبأسعار مناسبة، وحتى يكسبوا ثقة المشتري، ونظراً للقيود الأمنية على بيع مثل هذه الأجهزة، يتم دفع ثمن السلعة عند استلامها، فلا يتم توفير غير رقم هاتف محمول مع صورة السلعة ووصف لأهم مميزاتها.

رابعاً: أبرز ملامح حروب التواصل الاجتماعي على المستوى الإقليمي سيطرت على حروب التواصل الاجتماعي، إقليمياً، عدد من القضايا الرئيسية أهمها انقسام المنطقة العربية حول الدور السياسي للتيار الإسلامي، بالإضافة إلى تصاعد دور الحركات الإرهابية في منطقة الشرق الأوسط

وبخاصة تنظيم الدولة الإسلامية، فضلاً عن الاعتداءات الإسرائيلية المتكررة على الفلسطينيين، وهو ما يتضح فيما يلي:

1- حروب فكرية بين التيارات السياسية سادت خلال الفترات الماضية، ومازالت، حرب افتراضية على مواقع التواصل الاجتماعي كان محورها الإسلاميون عموماً ودولة قطر خصوصاً، فقد مثّل الموقف القطري من دعم الإسلاميين وجماعة الإخوان مجالاً للنقد والهجوم على مواقع التواصل الاجتماعي، وظهرت العديد من الهاشتاجات ما بين تأييد أو رفض للموقف القطري، ومنها مثلاً هاشتاج "#قطر _ تدعم _ الإرهاب"، وهو الأمر الذي رفضه أنصار قطر وبخاصة من الإسلاميين واتخذوا موقف المدافع عنها باعتبارها داعماً رئيسياً للثورات العربية، وظهرت كثير من الهاشتاجات التي تسئ لبعض الدول العربية.

2- مواجهة التنظيمات الإرهابية فقد مثّل تنظيم الدولة الإسلامية المعروف إعلامياً ب"داعش" محور اهتمام مواقع التواصل الاجتماعي، خاصةً بعد الاستراتيجية الإعلامية التي اتبعها من خلال مواقع التواصل الاجتماعي، ونجح من خلالها في تجنيد العديد من الأفراد في المنطقة العربية، ونجح أيضاً في خلق صورة ذهنية عن بشاعة أفعاله، ساعدته في دخول بعض القرى العراقية دون مقاومة تذكر.

وقد شهدت مواقع التواصل حرباً حقيقة منظمة خاصة مع تزامن الضربة الأمريكية لمواقع "داعش"، حيث كشفت جريدة ال"تليجراف" عن أن الخارجية الأمريكية دشنت عدة حسابات على مواقع التواصل الاجتماعي لمواجهة حملة "داعش" لتجنيد مزيد من الأفراد، حيث تعمل هذه الحسابات بلغات عدة منها الإنجليزية والعربية والأردو والصومالية وتقوم ببث صور ومقاطع فيديو تكشف الدمار الذي تخلفه الغارات الجوية التي تستهدف ما تقول إنه مواقع "الدولة الإسلامية" في العراق وسوريا كتحذير للشباب الذين يفكرون في الانضمام إليها [55].

3- نشر الفكر المتطرف وتجنيد الأفراد تعتبر مواقع التواصل الاجتماعي أداة رئيسية للجماعات الإرهابية لنشر أفكارها المتطرفة والبحث عن مجندين لها، ويعتبر موقع "فيس بوك" من أكثر وسائل التواصل الاجتماعي استخداماً في تجنيد المتطرفين، حيث تقوم الجماعات الإرهابية بإنشاء مجموعة Group على "فيس بوك" لاجتذاب المتوافقين فكرياً معها، وذلك من خلال تبني قضية إنسانية، كدعم الفلسطينيين أو الدفاع عن الإسلام، أو الدعوة للجهاد في أفغانستان ومالي والعراق وسوريا. وقد لوحظ أنه مع زيادة عدد الأعضاء المنتمين لأي من هذه المجموعات، فإن المواد الجهادية يتم وضعها تدريجياً عليها بطريقة لا تستهجن الأفعال الجهادية أو تدينها، حتى لا تنتهك سياسة "فيس بوك"، ثم يتم بعد ذلك توجيه أعضاء المجموعة مباشرة إلى المواقع أو المنتديات المرتبطة بالجماعة الإرهابية [56]. وهناك مئات من الصفحات على موقع ال"فيس بوك" التي تدعو للجهاد مثل صفحات "الجهاد في سبيل الله" و"الجهاد في سوريا" و"أريد الجهاد"، و"تأخرنا عن الجهاد".

إلى جانب ذلك، تعتمد الجماعات الإرهابية والمتطرفة على هذه المواقع في نشر المعرفة بكيفية تصنيع القنابل، وتنفيذ العمليات الإرهابية، وذلك من خلال نشر العديد من مقاطع الفيديو على

موقع ال"يوتيوب" خاصة بكيفية تصنيع الأسلحة والمتفجرات والعبوات البدائية أو كيفية استخدام بعض الأسلحة مثل ال"كلاشينكوف[57] ". بل تقوم صفحات أخرى بالإتجار في الأسلحة علناً عبر صفحات ال"فيس بوك" مثل صفحة " أسلحة دفاع عن النفس". كما انتشر عدد من الصفحات التى تعرض أنواعاً مختلفة من الأسلحة مثل طبنجات الرصاص الحي والصوت والرشاشات بالإضافة إلى المطاوي والسيوف والكف المدبب، وتتراوح أسعار الطبنجات الرامبو ال9 مللي بين 850 جنيها و15 ألفاً. كما تعرض هذه الصفحات بندقيات خرطوش أتوماتيك تركية الصنع بنحو 12 ألف جنيه[58].

وانتشار هذا النوع من المعرفة على الإنترنت، هو الأساس لانتشار نوع جديد من الإرهاب مؤخراً في مصر وغيرها من الدول في المنطقة، "الذئب المنفرد" Lonely wolf، وهو الإرهابي الذي يعتمد على مواقع التواصل الاجتماعي والإنترنت في الحصول على المعلومات والتدريبات للقيام بعمليات إرهابية فردية وليس في إطار تنظيم، وفي أن يحصل أيضاً على الطريقة التي يتم بها صناعة الأسلحة والمتفجرات وأن يقوم بشراء بعضها من خلال الصفحات الاجتماعية.

إلى جانب ذلك، تستخدم الجماعات الإرهابية مواقع التواصل الاجتماعي كأداة لتحديد أهدافها والتعرف عليها ومراقبة تحركاتها، خاصة في إطار عمليات الاغتيالات التي تطال بعض رموز الأجهزة الأمنية أو السياسية في الدول المستهدفة، وذلك إما بمراقبة من يمتلك حسابات على تلك المواقع، أو مراقبة دائرة أصدقائهم ومعارفهم للوصول إليهم، وجمع البيانات اللازمة عن تحركاتهم، وتوفير الوقت والجهد اللازمين للقيام بذلك على أرض الواقع، وأيضاً ضمان سرية المراقبة[59].

وفي هذا السياق، يمكن فهم دعوة الرئيس "عبد الفتاح السيسي" للأمم المتحدة؛ لغلق الصفحات التكفيرية على مواقع التواصل الاجتماعي، والصفحات الخاصة بالجماعات الإرهابية[60]. وقد لوحظ أنه على الرغم من قيام موقع "تويتر" وال"فيس بوك" بغلق بعض هذه الصفحات والحسابات، إلا أنه سرعان ما تبدأ في الظهور من جديد، ومن ذلك الحسابات الخاصة بتنظيمات جبهة النصرة و"داعش" وأنصار الإسلام وأنصار الشريعة والقاعدة على "تويتر"، فهي تمتلك عدداً أكبر من الحسابات، ويتم فتح حساب جديد بدلاً عن الحساب الذي يتم إغلاقه، سواء بنفس الاسم السابق أو باسم جديد، وتبدأ الميكنة الإعلامية للحركات الجهادية في الإعلان عنها من جديد، وهو ما يضع جدوى الإغلاق في موضع التساؤل.

4- ربط الجماعات المتطرفة بعضها ببعض تعتبر مواقع التواصل الاجتماعي بصفة خاصة، والتطبيقات الاجتماعية بصفة عامة أحد أدوات التربيط بين الجماعات الإرهابية؛ حيث يستخدمها أعضاء التنظيمات الإرهابية في عمليات التواصل فيما بينهم وفي تبادل المعلومات، خاصة مع انتشارها في مناطق جغرافية متباعدة وارتباطها تنظيمياً أو فكرياً ببعضها البعض؛ فتصبح مواقع التواصل أحد الأدوات التي تسهل عملية الاتصال. فضلاً عن استخدامها في الحصول على التمويل اللازم للقيام بعمليات إرهابية من خلال المتعاطفين مع هذه التنظيمات،

لاسيما في ظل سهولة استخدام تلك المواقع لتحويل التبرعات والدعم المالي، مع عدم إمكانية التحقق من هوية متلقي تلك التبرعات في بعض الأحيان.

وإلى جانب الدعم المادي، تحصل تلك الجماعات على الدعم المعنوي أيضاً من خلال مواقع التواصل الاجتماعي؛ حيث شهدت بعض الصفحات الإلكترونية ما أسماه البعض "البيعة الافتراضية" لزعيم تنظيم "داعش" من جانب آلاف السلفيين الجهاديين، وجاء ذلك على إثر إعلان الناطق باسم التنظيم عن تأسيس "دولة الخلافة"، في المناطق التي يوجد فيها التنظيم في العراق وسوريا. وظهرت صفحات على شبكات التواصل الاجتماعي من بينها "بيعة أمير المؤمنين أبو بكر البغدادي"، و"إعلان الولاء الشرعي لأمير المؤمنين أبو بكر البغدادي" وغيرها. وهو الأمر الذي ساهم في انتشار التنظيم وزيادة عدد مؤيديه عبر العالم الافتراضي[61].

5- أداة رئيسية في المواجهات العربية - الإسرائيلية عادةً ما يصاحب الاعتداء الإسرائيلي على الفلسطينيين حملة إعلامية يشنّها الناشطون الفلسطينيون والعرب لفضح انتهاكات الاحتلال الإسرائيلي، ولعل المواجهة الأخيرة التي دارت رحاها في سبتمبر 2014، شهدت تواجداً مكثفاً للشبكات الاجتماعية لفضح هذه الانتهاكات؛ حيث بادر الناشطون بنشر صور وفيديوهات للقصف الإسرائيلي على غزة. وفي المقابل قام الجيش الإسرائيلي بنشر صور وفيديوهات مضادة توضح تعرض إسرائيل للقصف من قبل الفلسطينيين وتوضح حقهم في الدفاع عن أنفسهم. وتبارى كل فريق لكسب تأييد الرأي العام الدولي لصالحه. وفي المقابل انطلق على موقع "تويتر" وغيره من المواقع هاشتاجان رئيسيان هما "#GazaUnderAttack" و"#IsraelUnderFire" وحاول كل فريق منهما توضيح المعاناة التي يتعرض لها جراء القصف؛ حيث ألقت الحرب بظلالها على مواقع التواصل الاجتماعي، ونشبت حرب افتراضية توازي الحرب الحقيقية.

الفصل السادس: كيف يمكن التغلب على التهديدات التي تطرحها الشبكات الاجتماعية؟

بعدما استعرضنا الجانب السلبي للشبكات الاجتماعية، والتهديدات التي تطرحها؛ حان الوقت لمعرفة كيفية تجنبها، وتجنيب الآمنين والمدنيين سلبياتها؛ وذلك من خلال مطالعة بعض النماذج الدولية وطرق تعاملها مع تهديدات الشبكات الاجتماعية، بهدف التوصل إلى نموذج يضمن للفرد أمنه، وقبل ذلك يضمن له حريته وخصوصيته.

أولاً: النماذج الدولية في التعامل مع تهديدات مواقع التواصل الاجتماعي وفيما يلي بعض أبرز هذه النماذج، سواء كانت من الدول الديمقراطية مثل الولايات المتحدة الأمريكية وبريطانيا، أو الدول الديكتاتورية مثل الصين وإيران[62]:

1- الولايات المتحدة: برنامج بريزم PRISM بموجب قانون حماية أمريكا Protect America Act[63] الصادر في عام 2007، تم إنشاء برنامج سري يدعى US-984XN ويُعرف إعلامياً باسم PRISM ويعمل هذا البرنامج على مراقبة المعلومات على الفضاء الإلكتروني، ومراقبة الاتصالات الحيّة والمعلومات المخزنة التي تخص أشخاصاً محددين داخل الولايات المتحدة وخارجها. يستطيع هذا البرنامج الحصول على معلومات تتضمن رسائل البريد الإلكتروني، ومحادثات الفيديو والصوت، والصور، والاتصالات الصوتية ببروتوكول الإنترنت، وعمليات نقل الملفات، وإخطارات الولوج وتفاصيل الشبكات الاجتماعية[64]. وبموجب قانون حماية أمريكا، فإنه بمجرد موافقة أحد القضاة السريين ب "محكمة مراقبة الاستخبارات الخارجية"، يحق لوكالة الأمن القومي الأمريكي NSA أن تطلب من الشركات العاملة في مجال الإنترنت مثل "ياهو" و"فيس بوك" و"جوجل" و"أبل" و"مايكروسوفت" وغيرها، بيانات تتعلق بمستخدمين محددين[65].

إلى جانب ذلك، ينظم مراقبة التطبيقات الاجتماعية في الولايات المتحدة، قانونان آخران هما: المادة 207 من قانون مراقبة الاستخبارات الخارجية The Foreign Intelligence Surveillance Act والمادة 215 من القانون الوطني Patriot Act؛ حيث يخول القانون الأول السلطة لوكالة الأمن القومي الأمريكي لجمع المعلومات الخاصة بالتواصل الإلكتروني من برنامج "بريزم" وغيره من البرامج عبر شركات الإنترنت، ويخول الثاني السلطة لها لجمع المعلومات العملاقة الخاصة بالاتصالات الهاتفية من شركات الاتصالات[66]. وتحصل وكالة الأمن القومي على هذه البيانات إما مباشرة من خلال خطوط Upstream التي تعمل على سحب البيانات مباشرة من الكابلات البحرية التي تحمل المعلومات، أو من خلال الخوادم التي يتم تخزين هذه البيانات عليها لشركات أمريكية، مثل برنامج "بريزم" للحصول على المعلومات من الشركات [67].

وفي تقرير صادر عن وزارة الأمن الداخلي في نوفمبر 2012 بعنوان "Privacy Compliance Review مراجعة الالتزام بالخصوصية"، تأكيد على أنه منذ يونيو 2010 على الأقل ومركز العمليات التابع للوزارة يقوم بعمليات متابعة لمواقع التواصل الاجتماعي ومواقع الإنترنت، والتي تتضمن الاطلاع المنتظم على "منتديات الإنترنت المتاحة للعامة والمدونات ومواقع الإنترنت العامة"؛ وذلك بهدف مساعدة وزارة الأمن الداخلي في التحرك السريع لمواجهة الأزمات

والكوارث، ومساعدة أجهزة المخابرات الأمريكية ووكالة الأمن القومي على مواجهة حالات الطوارئ والعمل على خلق قنوات اتصال للتعامل السريع مع الكوارث[68]. وقد صرح مسئول في وزارة الأمن الداخلي، مطّلع على برنامج المتابعة، إن الهدف الوحيد منه هو تمكين مسؤولي مركز القيادة من أن يكونوا في تواصل دائم مع الوسائل المختلفة في عصر إعلام الإنترنت، حتى يصبحوا مدركين للأحداث الرئيسية التي ربما يتعين على الوزارة أو أجهزتها التعامل معها[69].

(صورة توضح الطريقة التي تجمع بها وكالة الأمن القومي الأمريكي البيانات عبر الإنترنت) ولما كان الاعتماد على الأجهزة المحمولة يتزايد، مثل الهاتف المحمول والحاسب اللوحي وغيرهما، فقد أصبحت هدفاً للإدارة الأمريكية، لما يمكن أن توفره من معلومات حول مستخدميها. خاصةً إذا كان هذا المستخدم هدفاً لأحد الأجهزة الأمريكية؛ حيث يمكن اختراق بعض تطبيقات الهاتف المحمول ومعرفة مكان هذا الشخص، وسرقة المعلومات الموجودة على هاتفه. وكذلك تستفيد الإدارة الأمريكية أيضاً من تطبيقات مواقع التواصل الاجتماعي للحصول على كافة البيانات المُخزنة في حسابات المُستخدمين، مثل العمر والجنس والميول ومكان التواجد والمُستوى العلمي وغيرها[70].

ومن أبرز التطبيقات التي اعتمدت عليها الولايات المتحدة لاختراق الهاتف المحمول هو تطبيق Angry Birds أو الطيور الغاضبة، وهي لعبة ذائعة الصيت على الأجهزة المحمولة واللوحية، فقد كشف تقرير نشرته صحيفة "الجارديان" البريطانية، أن وكالة الأمن القومي الأمريكية تقوم بتطوير تقنيات تسمح لها باستغلال تطبيقات الهواتف الذكية للوصول إلى معلومات خاصة بالمُستخدمين[71] ، فقد سرب "سنودن" وثائق تؤكد استهداف وكالة الاستخبارات الأمريكية CIA بيانات الهاتف المحمول للمُستخدم وذلك لجلب معلومات عن الإرهابيين وأهداف استخباراتية أُخرى[72] ؛ حيث أنفقت ما يزيد على مليار دولار لصالح برامج التجسس الخاصة باستهداف الهواتف الذكية [73].

ولتوضيح قُدرة برامج الوكالة الأمريكية؛ أشار تقرير "الجارديان" إلى أنه وبمجرد قيام المُستخدم برفع صورة إلى وسائل التواصل الاجتماعي باستخدام هاتفه الذكي، تستطيع الوكالة جمع معلومات مثل جهات الاتصال في هاتف المُستخدم، وعناوين البريد الإلكتروني، وموقع المُستخدم[74].

2- بريطانيا: نموذج SOCMINT صرّح لأول مرة "تشارلز فار" المدير العام لمكتب الأمن ومكافحة الإرهاب في بريطانيا في يونيو 2014، بأن "الحكومة البريطانية تراقب مواقع التواصل الاجتماعي والتي تشمل ال"فيس بوك" و"تويتر" و"يوتيوب" بالإضافة إلى الإيميلات الشخصية للمواطنين البريطانيين باعتبارها اتصالات خارجية"[75]. وفي أعقاب أحداث الشغب التي شهدتها بريطانيا في أغسطس 2011، قامت الشرطة البريطانية في هذه الأثناء بمراقبة مواقع التواصل الاجتماعي بهدف التحرك عند الضرورة، واعتقلت السلطات في إنجلترا وأسكتلندا أكثر من 12 شاباً بتهمة استخدام الإنترنت والرسائل النصية للتحريض على أعمال الشغب[76].

وقد استخدمت الحكومة البريطانية برنامج (SOCMINT)Social Media Intelligence بهدف تحليل البيانات الموجودة على مواقع التواصل الاجتماعي دون الحاجة لاختراق خصوصية المستخدمين أو الدخول على رسائلهم الخاصة؛ وذلك بالاعتماد على مجموعات عمل تقوم برصد وتحليل مواقع التواصل بهدف الخروج بمؤشرات إحصائية حول المستخدمين النشطين والمؤثرين على مواقع التواصل الاجتماعي، وكذلك بمؤشرات معلوماتية خاصة بعمليات الحشد والتعبئة التي تقوم بها بعض الحركات الجهادية على مواقع التواصل الاجتماعية[77].

كما قامت وزيرة الداخلية البريطانية "تريزا ماي" بطرح مشروع قانون في نوفمبر 2014، يلزم شركات الاتصالات بتسليم معلومات للشرطة حول هوية الأشخاص الذين يستخدمون الحواسيب أو الهواتف المحمولة في وقت ما، بهدف تدعيم الأمن القومي لبريطانيا؛ فوفقاً لمشروع القانون المقترح والمقدم تحت لافتة قانون الأمن ومكافحة الإرهاب، فإن الشركات المزودة للخدمة عليها أن تحتفظ بالبيانات التي تربط بين الأجهزة والمستخدمين[78].

وقد كشف مسؤولون في وزارة الدفاع البريطانية السبت 31 يناير 2015 عن إنشاء وحدة مختصة في الحرب الإلكترونية، مؤلفة من خبراء شبكات التواصل الاجتماعي، لخوض الحروب المعلوماتية، هي الكتيبة 77 وتتكون من جنود نظاميين واحتياط، تتمركز في بلدة "هيرميتاج" فى "بيركشاير". ومن المقرر أن تبدأ نشاطها فى أبريل من نفس العام، ويصل عدد الجنود فيها إلى 1500 جندي، ينتمون إلى كتائب مختلفة في الجيش البريطاني، القاسم المشترك بينهم هو خبرتهم في مجال مواقع التواصل الاجتماعي وشنّ الحرب النفسية من خلالها. وقال متحدث باسم وزارة الدفاع البريطانية إن الوحدة ستلعب دوراً أساسياً في تمكين المملكة المتحدة من خوض حرب عصر المعلومات. "وتم تشكيل الكتيبة 77 لجذب وتطوير القدرات الحالية لمواجهة تحديات الحرب الحديثة". وتتلخص مهمة الكتيبة 77 في متابعة الأخبار المتبادلة عن طريق المواقع والهواتف الذكية، ومحاولة التحكم في ما يخص الجيش البريطاني منها[79].

3- الصين: الجدار الناري العظيم تعتبر الصين هي النموذج الأبرز والأقوى في تشديد الرقابة، ليس فقط على الشبكات الاجتماعية، ولكن أيضاً على الإنترنت بصفة عامة؛ فشبكة الإنترنت في الصين أشبه بشبكة داخلية Intranet، تقوم الحكومة فيها بدور مقدم الخدمة ومن ثم التحكم في كل البيانات الموجودة على الإنترنت. وعلى إثر مصادمات وأحداث عنف شهدتها البلاد عام 2009 اندلعت بين مسلمي "الإيجورا" والشرطة في مدينة "أورمتشي" التي تقع شمال غرب الصين، اتخذت الحكومة الصينية قراراً بغلق مواقع التواصل الاجتماعي "فيس بوك" و"تويتر" و"يوتيوب" و"بلوجر"، إضافةً إلى مواقع أخرى منها محرك بحث "جوجل"؛ حيث تعتبر حكومة الحزب الشيوعي الحاكم نفسها مسؤولة أخلاقياً عن حماية مواطنيها من التعرض لما تسميه الغزو الثقافي الغربي. كما أنه قد تكون هناك عوامل أخرى، من بينها إقفال الباب أمام محاولة الغرب لاستخدام هذه المواقع في إثارة الاضطرابات السياسية ضد الدولة الصينية؛ لذا تم بناء مشروع ما، يسمى بجدار نار الصين العظيم The Great Firewall of china أو ما يعرف رسميًا

باسم مشروع الغطاء الذهبي Golden Shield، ويعد أحد أكثر المشاريع تقدماً في العالم[80] ، فيما يتعلق بتقنية مراقبة الإنترنت وحجب المواقع الغير مرغوب بها.

ومن ناحية أخرى، توفر الصين لمواطنيها مواقع بديلة للمواقع المحجوبة مثل محرك البحث "بايدو" وموقع "يوكو" لمقاطع الفيديو وموقع "ويبو" للتغريدات القصيرة وموقع "بلوج سينا" للمدونات.

ورغم ما تمارسه الصين من محالات لحجب مواقع التواصل إلا أن المستخدمين يتحايلون على ذلك بطرق عديدة، وللمفارقة فإنه وبحسب إحصائيات eMarketer فإن هناك 35.5 مليون مستخدم نشط من الصين على تويتر حتى عام 2012؛ حيث يلجأ المستخدمون إلى أدوات مثل VPN لتجاوز الحجب، ويمكن أحياناً نشر التغريدات عبر تطبيقات خارجية مثل TweetDeck وغيرها [81].

4- إيران: التضييق على استخدام الإنترنت ويعتبر السجل الإيراني حافلاً بالعديد من حالات إغلاق مواقع التواصل الاجتماعي؛ حيث تعمل السلطات الإيرانية بانتظام على منع الوصول إلى شبكات التواصل الاجتماعي خصوصاً "تويتر" و"فيس بوك" ومواقع أخرى تعتبر غير إسلامية أو تضر بالنظام الإسلامي. وقد بدأ ذلك منذ عام 2009 في أعقاب ما تم تسميته بالثورة الخضراء أو ثورة "تويتر" عقب احتجاجات واسعة شهدتها البلاد اعتراضاً على نتيجة الانتخابات الرئاسية؛ حيث قام الناشطون السياسيون بعرض انتهاكات النظام الإيراني ضد المتظاهرين باستخدام مواقع التواصل الاجتماعي وبخاصة موقعي ال"يوتيوب" و"تويتر"، متغلبين بذلك على التعتيم الإعلامي الذي فرضه النظام الإيراني.

ولم ينته الأمر عند مواقع التوصل، بل امتد ليشمل تطبيقات الموبيل؛ ففي سبتمبر 2014 أمهل القضاء الحكومة شهراً لحظر شبكات الاتصال المجانية مثل "فايبر" و"تانجو" و"واتس آب" بسبب رسائل مهينة وجهت لمسؤولين في الجمهورية الإسلامية[82]. ورغم ذلك يستخدم بعض الشباب الإيراني تقنيات تسمح لهم بالولوج إلى الشبكات الاجتماعية رغم إغلاق الحكومة الإيرانية لها، وهو ما دفع رئيس الشرطة في إيران "إسماعيل أحمدي مقدم" إلى الإعلان عن إصدار "برنامج معلوماتي ذكي" يسمح ب"مراقبة ذكية لمواقع التواصل الاجتماعي" بدلاً من حجبها بالكامل[83]. ليشكل تحولاً جديداً في الطريقة التي تتعامل بها إيران مع مواقع التواصل الاجتماعي. كما تسعى في طريق آخر على غرار الصين، لإنشاء شبكة إنترنت وطنية منفصلة عن شبكة الإنترنت العادي، وسوف تعمل بصورة أسرع من الشبكة العادية، كما تشمل الخطة أيضا إنشاء محرك بحث وطني.

ومن خلال العرض السابق يتضح لنا أن الدول الديمقراطية قد نظرت إلى الشبكات الاجتماعية باعتبارها سلاحاً ذا حدين، قد يُستخدم فيما هو مفيد مثل التعامل السريع أوقات الأزمات والكوارث، وقد يستخدم لتهديد الأمن القومي من خلال التمويل غير المشروع أو تجنيد إرهابيين أو تخطيط لمظاهرات واحتجاجات أو إثارة للرأي العام ونشر الإشاعات. في حين نظرت إليها النظم الشمولية على أنها شر في حد ذاتها، ولكنه لابد منه، بسبب الانتشار المتزايد لها، فعملت الصين على إنشاء شبكات تواصل اجتماعي صينية مغلقة، وإغلاق الشبكات الدولية مثل ال"فيس

بوك" و"تويتر"، مع تشديد الرقابة على جميع المحتويات على شبكة الإنترنت. وعلى نفس خطى الصين تسير إيران، في رغبة منها لتضييق الخناق على الناشطين السياسيين والمعارضين ومراقبة محتوى الإنترنت الذي قد يشكل تهديداً للنظام السياسي الإسلامي الإيراني، ومن ثم فقد اتفق كلا النظامين الديمقراطي والشمولي على ضرورة إحكام الرقابة والسيطرة على الشبكات الاجتماعية كلٌ على طريقته.

ثانيا: هل الحفاظ على خصوصية الأفراد يشكل ضرورة أمنية؟

تكشف العديد من الخبرات الدولية عن أن عملية تقنين التطبيقات الاجتماعية ليست عملية سهلة، رغم الاعتقاد السائد بأن تدخل الدولة وإحكام قبضتها الأمنية على كافة وسائل الاتصالات يساعد في الكشف المبكر عن الجرائم والعمليات الإرهابية ويحافظ على الأمن القومي. لكن هل الحفاظ على خصوصية وسرية البيانات الشخصية وعدم التجسس عليها أو مراقبتها ولو جزئياً يساعد في الحفاظ على الأمن القومي؟. لعل الإجابة على هذا التساؤل تكون ب "نعم"، وذلك لأن انتهاك الخصوصية والحريات بصورة عامة دون وجود ضوابط وقيود تحدّ من هذه العملية قد يتسبب في العديد من المشكلات التي تهدد أمن النظام الحاكم، بل وأمن الدولة ككل، ومنها ما يلي[84]:

1 - التوجه نحو العمل السري: فالانتهاك التام لخصوصية الأفراد وتسجيل كافة بياناتهم على الشبكات الاجتماعية والاتصالات الهاتفية، قد يؤدي في النهاية إلى التوجه نحو العمل السري بعيداً عن أعين الدولة وأجهزة الأمن، وهو ما يصعّب من عملية اكتشاف الجرائم حتى بعد وقوعها، وتأخير عملية القبض على المجرمين، ومن ثَم يجب ترك هامش للحرية الحقيقية حتى يسلك الأفراد الطرق المعلنة في التعبير عن مطالبهم وأفكارهم دون خوف من رقابة أو تسجيل للاتصالات.

2 - اختلال التوازن التقليدي بين القوى السياسية: حيث يرتبط مفهوم الخصوصية ارتباطاً وثيقاً بالديمقراطية، فهي بمنزلة عقد غير مكتوب بين المواطنين والسلطة في البلدان الديمقراطية. ولعل الأزمة الكبرى في تقنيات مراقبة الجمهور أنها لا تؤدي فقط لمنع حرية الرأي والتعبير، ولكنها تؤدي أيضاً إلى منع المجتمع المدني من المعارضة السلمية، وإمكانية اللجوء إلى العنف، أو أنها قد تحول دون الحفاظ على توازن القوى مع السلطة الحاكمة، وعلاوة على ذلك، فإن هذه التقنيات تُضعف المجتمع المدني نفسه، من خلال تقويض وجود الخصوصية والثقة داخل الدولة، وهما من المحددات الأولية لتوازن القوى بين المواطن والدولة[85].

3 - تهديد سلامة الرموز السياسية: ففي ظل حالة عدم الخصوصية التي أصبح يتميز بها الإنترنت فإن سلامة الرموز السياسية أصبحت معرضة للخطر بكل سهولة، فتواجده على موقع مثل ال"فيس بوك" و"تويتر" أو غيره يوفر عنه كثيراً من المعلومات الشخصية التي قد تستخدمها بعض الحركات في تنفيذ عمليات إرهابية، سواء من خلال معرفة أماكن تواجده الحالية واستهدافه فيها، أو تحديد شبكة الأقارب واختطاف أحدهم لممارسة نوع من الضغوط، أو من

خلال معرفة الماركات التي يفضلها عبر الصفحات التي يشترك فيها على الشبكات الاجتماعية واستغلال هذه المعلومات في الإيقاع به.

4 - تسريب البيانات والمعلومات بهدف التشويه: حيث شهدت مصر في الفترة الأخيرة تسريب العديد من المكالمات الشخصية سواء لرموز سياسية أو عسكرية، بل قامت برامج تليفزيونية بإذاعة هذه التسريبات، وتم توظيفها بصورة تضرّ بصاحبها أو بالمؤسسة التي ينتمي إليها صاحب التسريب، ومن ثم فإن عملية انتهاك الخصوصية بصورة كاملة قد تؤدي إلى انقلاب السحر على الساحر، فقد يتم انتهاك خصوصية القائم على عملية التسجيل شخصياً، ويصبح مُنتهَك الخصوصية بعد أن كان مُنتهِكاً لها، ومن ثَم فإن التساهل في عملية التسجيل والتسريب قد يؤدي إلى تسهيل عملية التسجيل والتسريب للقادة السياسيين والعسكريين، لذا يجب وضع قيود صارمة على عمليات التسجيل وانتهاك الخصوصية.

5 - تشجيع سوق البرامج المجانية لانتهاك الخصوصية: فتوجه الدول والأنظمة الحاكمة نحو هذا النوع من البرامج التي تراقب وتسجل للأفراد اتصالاتهم ومكالمتهم يعمل بطريقة مباشرة على إنعاش سوق التجسس اقتصادياً، وهو ما يساعد في توفير برامج مجانية يمكنها انتهاك خصوصية الأفراد على شبكة الإنترنت، وتتوافر هذه البرامج بكثرة حالياً، وبخاصة لموقع التواصل الاجتماعي "تويتر"؛ حيث توفر معلومات دقيقة عن الحساب الإلكتروني المرجو انتهاك خصوصيته منذ نشأته حتى الوقت الحالي، سواء من حيث الأماكن الجغرافية لتواجده، أو شبكة الأقارب الخاصة به، أو الساعات التي يتواجد فيها على الإنترنت، أو الصفحات التي يقرأها باستمرار وغيرها من المعلومات.

ثالثاً: سياسات مقترحة لتفادي تهديدات الشبكات الاجتماعية تم تقديم مقترح هذه السياسات في الورقة التي تم نشرها بسلسلة "بدائل" الصادرة عن مركز الأهرام للدراسات السياسية والاستراتيجية في أبريل 2015، والتي جاء فيها أن الخبرات الإقليمية والدولية تكشف عن ثلاثة بدائل لتفادي التهديدات الناجمة عن الشبكات الاجتماعية. شأنها شأن غيرها من الدول التي يتزايد فيها استخدام هذا النوع من الشبكات، على نحو يعالج بصورةٍ ما الجدلية الثلاثية المتعلقة بالخصوصية والحريات والأمن، وكل بديل منها لا يحقق توازناً حقيقياً بين هذه المكونات الثلاثة، وقدرة الدولة على اتباع أي منها يتطلب توافر مجموعة من الشروط، وسيتم مناقشة كل منها على حدة.

1- الرقابة الكاملة نتيجةً للظواهر السلبية التي أفرزتها الشبكات الاجتماعية، سواء كانت سياسية أو اقتصادية أو اجتماعية أو إعلامية فإن مراقبتها أمر رئيسي للمحافظة على الأمن القومي للدول؛ حتى لا تصبح ساحة للعمليات الإرهابية أو مجالاً للمنظمات الإجرامية والمافيا، ومن ثم العمل على سرعة كشف الجرائم قبل أو فور وقوعها، ومحاصرة نطاق انتشار الإرهاب، ووقف الصفحات التي تبث الكراهية والعنف ونبذ الآخر.

وفي هذه الحالة يتعين على الدولة أن تسيطر على كافة خدمات الإنترنت، وأن تمتلك وحدها السيطرة على جميع بيانات الإنترنت، بما فيها خوادم الشركات العملاقة الغير موجودة في مصر مثل ال"فيسبوك" و"جوجل" و"تويتر". بالإضافة إلى الخوادم الخاصة بتطبيقات الموبيل مثل

ال"واتس آب" و"فايبر". بل وأن تتبنى نموذج الصين في بناء جدار ناري للعمل على كشف الثغرات الأمنية منعاً لاستخدامها من خلال توظيف مئات أو آلاف الشباب الذين يعملون بمثابة كتائب إلكترونية تعمل على توجيه الرأي العام الإلكتروني، وأن تمتلك برامج تحليل عملاقة، تعمل على رصد كل ما يثار على الإنترنت وتحليله، بهدف سرعة التعامل معه.

ويمكن الإشارة في هذا الصدد إلى طلب الهند من مصنع أجهزة الهواتف المتعددة الوسائط "بلاك بيري" وكافة مزودي خدمات الإنترنت، من بينهم "سكايب" و"جوجل"، بإنشاء خوادم (سيرفر) محلية للسماح بوصول أجهزة الاستخبارات الهندية إلى البيانات المتداولة عبر الشبكة [86]. كما أصدرت دولة الإمارات العربية المتحدة قراراً بتعليق خدمات "بلاك بيري" لوجود "عواقب خطيرة على الأمن الاجتماعي والقضائي والأمن الوطني".، وقد تم حل الأزمة بعدما منحت شركة "بي جي بي" المسئولة عن تشفير بيانات خدمات أجهزة "بلاك بيري" السلطات الإماراتية حق الوصول إلى مفتاح شفرة خدمات المراسلة الفورية "الماسنجر"؛ تنفيذًا للاتفاق المبرم مع الشركة الكندية المصنعة للهاتف المذكور "ريسيرتش أن موشن" دون الكشف عن تفاصيل[87].

2- رفع الوعي بين المواطنين كبديل عن الرقابة وذلك من خلال رفع يد الدولة عن جميع المحادثات التي تتم سواء عبر مواقع أو تطبيقات التواصل الاجتماعي، والحفاظ على سرية وخصوصية البيانات والاتصالات الشخصية وعدم التجسس عليها أو اختراقها أو تسريبها للعامة. مع العمل على رفع وعي المواطنين، وتوعيتهم بالتحديات والتهديدات التي تطرحها الشبكات الاجتماعية، وعمليات النصب والاحتيال التي قد يتعرضون لها، والمخاطر الفكرية الناجمة عن تواجد الحركات الإرهابية عليها.

ويمكن تحقيق ذلك من خلال إفساح المجال لوسائل الإعلام التقليدية لمحاربة التشدد الذي تبثه بعض الصفحات الاجتماعية، من خلال برامج تليفزيونية تعرض ما يدار على هذه الصفحات، ويقوم المتخصصون وأصحاب الرأي والفكر بالرد على الحجج التي يتم تداولها، وأن يتم التعويل على الشباب المصري للإبلاغ عن أي حالات اشتباه في عمليات غير قانونية أو متطرفة تتم عبر هذه الشبكات؛ ومن ثم يمكن محاصرة التهديدات التي تأتي عبر هذه الشبكات.

ولكن المشكلة الرئيسية في أن عملية رفع الوعي تأخذ وقتاً قد تنجم فيه تهديدات خطيرة، وجديدة، فضلاً عن اعتماد الحركات المتشددة والعصابات الإجرامية على تقنية تكنولوجية متطورة، قد لا يعلمها كثير من مستخدمي الشبكات الاجتماعية التقليديين. فضلاً عن تحدي استجابة الشباب ومستخدمي الشبكات الاجتماعية في الإبلاغ عن حالات اشتباه لإساءة استخدام هذه الشبكات، ومن ثم يكون هذا البديل محل شك للتنفيذ.

3- الرقابة "المقننة" من خلال المعلومات "المعلنة" ويقصد بهذا البديل أن يتم تقييد وتقنيين الرقابة التي تمارسها مؤسسات الدولة على التطبيقات الاجتماعية بأنواعها المختلفة، من خلال مجموعة من القوانين المنظمة يتم صياغتها بما يتفق مع الدستور، وعلى نحو يضمن عدم انتهاك خصوصية الأفراد وحرياتهم إلا في الحالات التي تهدد الأمن القومي للدولة.

وكذلك إصدار قانون ينظم الحالات التي يمكن أن يتم فيها مراقبة الاتصالات الإلكترونية والهاتفية على سبيل الحصر، والتفرقة بين الحالات التي تندرج في نطاق تهديد الأمن القومي والتخابر الخارجي، وبين الحالات الداخلية التي تقوم بالتعبير عن آرائها في حرية تامة.

وذلك إلى جانب تبني سياسات خاصة بمتابعة وتحليل المعلومات المعلنة الموجودة على التطبيقات الاجتماعية بأنواعها المختلفة، وهو ما يتطلب توافر برامج متقدمة تكون قادرة على تجميع هذه المعلومات وتحليلها على نحو يسمح بتحديد مبكر لمصادر الخطر والتهديد. وتقدم كل من الولايات المتحدة الأمريكية وبريطانيا نموذجين في هذا السياق، كما سبق توضيحه.

بالإضافة إلى ذلك، يمكن لبعض الدول تبني مجموعة أخرى من السياسات تشمل ما يلي:

1 - تطوير قوانين تلزم شركات الإنترنت والاتصالات بتقديم المعلومات الخاصة بالمستخدمين محل الاشتباه للأجهزة الأمنية، بعد حصولها على إذن قضائي من المحكمة المختصة.

2 - توقيع بروتوكولات مع الشركات المشغلة للتطبيقات ومواقع التواصل الاجتماعية مثل ال"فيس بوك" و"تويتر" و"جوجل" وغيرهم، بمساعدة الدولة في ملاحقة المجرمين أو المتطرفين الذين يستخدمون مواقع التواصل الاجتماعي لأغراض إجرامية أو إرهابية، وذلك بعد حصولها على أذن من المحكمة المختصة.

3 - تطوير "ميثاق شرف" لمستخدمي مواقع التواصل الاجتماعي، وتفعيل دور الرقابة الشعبية على المحتويات الغير أخلاقية أو التي قد تهدد الأمن القومي.

4 - إعلان "قائمة سوداء" سنوية بالصفحات الموجودة على التواصل الاجتماعي والتي تحضّ على العنف والكراهية وتشجع التطرف والإرهاب.

5 - تفعيل مراكز الاستجابة للطوارئ المعلوماتية "سيرت"[88] وإسناد مهمة متابعة وتحليل الشبكات الاجتماعية إليها.

6 - إنشاء محكمة قضائية مختصة لأخذ موافقتها أولاً في كل الحالات التي ترغب فيها أجهزة الأمن في مراقبة أنشطة إلكترونية ما، سواء على الشبكات الاجتماعية أو البريد الإلكتروني أو الاتصالات الهاتفية.

7 - تفعيل دور البرلمان، وإعطاء اللجان المختصة الحق في عمل جلسات استماع لأجهزة الأمن حول أسباب قيامها بمراقبة أو تسجيل أحد الاتصالات الإلكترونية عبر الشبكات الاجتماعية، ومعرفة الظروف الأمنية التي دفعتها للقيام بذلك.

8 - اتباع مبدأ المصارحة والشفافية في المعلومات التي يستطيع الجمهور الاطلاع عليها بشأن عدد حالات المراقبة وأسبابها وأخطارها، دون التطرق للأسماء أو المناصب أو المواقع الجغرافية حفاظاً على السلامة الشخصية.

خاتمة

مع التزايد المستمر في استخدام الهواتف الذكية، وتوجه الشركات الكبرى مثل "سامسونج" لتوفير هواتف ذكية بأسعار مخفضة في إطار التمكين الرقمي للفئات المهمشة اجتماعياً أو محدودة الدخل؛ فإن ذلك سيعمل بالضرورة على رفع نسبة مستخدمي الإنترنت في العالم العربي؛ ومن ثم ارتفاع نسبة استخدام التطبيقات الاجتماعية وشبكات التواصل. وقد ينعكس ذلك على أنماط استخدام الشبكات الاجتماعية، سواء من خلال الهاتف المحمول أو أجهزة الكمبيوتر. سواء بصورة إيجابية أو بصورة سلبية. لتظهر أنماط جديدة غير متوقعة، قد يكون بعضها مفيداً وقد يتسبب البعض الآخر في تهديد الأمن القومي، أو على الأقل تكدير السلم العام في المجتمع أو تعريض حياة بعض الأشخاص إلى الخطر.

وقد حددت الدراسة عدة أنماط رئيسية لاستخدامات الشبكات الاجتماعية قد تهدد السلم العام. قد يختفي بعضها نتيجة الرقابة المنظمة على الشبكات الاجتماعية؛ مثل نشر الأفكار المتطرفة وتجنيد الأفراد والجرائم الإلكترونية كالتحرش أو الابتزاز والتجارة غير الشرعية كالمخدرات والرقيق الأبيض. إلا أن هناك أنماطاً أخرى لا تجدي الرقابة معها نفعاً؛ مثل نشر الإشاعات وإثارة الرأي العام والمظاهرات والاحتجاجات الإلكترونية والاستخدامات المسيئة للهاشتاجات. فهذه الطرق تحتاج إلى أدوات تعامل غير تقليدية، تتمثل في العمل على سرعة توضيح الحقائق قبل أن تتحول لإشاعات يصعب السيطرة عليها، وتحقيق العدالة بمفهومها الواسع حتى لا يحتاج المواطنون لتنظيم تظاهرات أو احتجاجات.

وأيضاً هناك أنماط أخرى قد تنشأ نتيجة التقدم التكنولوجي في هذا المجال، فقد ظهرت بعض التطبيقات الاجتماعية في الآونة الأخيرة مثل تطبيق Snapchat والذي يقوم المستخدم من خلاله بإرسال لقطات فيديو تُعرض مرة واحد وبعدها تختفي وتمحى من الهاتف ومن خوادم التطبيق أيضاً، بصورة قد تعوق عمل الأجهزة الأمنية خاصة عند تهديد أحد الشخصيات بالقتل أو خلافه من خلال هذا التطبيق، وصعوبة إثبات الجريمة على الفاعل. كما بدأ نوع جديد من الشبكات في الانتشار مثل شبكة Socialnumber والتي تخفي الهوية الحقيقية للمستخدمين، وتستعيض عن الأسماء بأرقام من 6 - 10 للتسجيل في الموقع، وبداية تبادل الأخبار والمعلومات في ظل هويات غير محددة أو معلومة الملامح.

وقد يؤدي هذا التطور في مجال الشبكات الاجتماعية إلى ظهور أنماط أكثر عنفاً من السابق ذكرها، في ظل مجهولية الهوية واختفاء البيانات والأدلة في نفس الوقت، بصورة تجعل أجهزة الأمن تتعامل مع أشباح على الشبكات الاجتماعية، وليس أفراداً لديهم هويات حقيقية. وهو ما دفع الصين لوضع مجموعة قوانين جديدة تجبر المستخدمين على استخدام الاسم الحقيقي لهم عند التسجيل على الإنترنت سواء لشبكات التواصل الاجتماعي أو برامج المحادثات الفورية أو المنتديات أو المدونات أو غيرها من التطبيقات. كما أنها تعاقب من يستخدم أسماء عامة كأسماء رؤساء الدول أو الزعماء أو غيرها. وإذا كان النموذج الصيني متطرفاً في إحكام القبضة على أنشطة الإنترنت، إلا أن خطوة إصدار قانون للتسجيل باستخدام الاسم الحقيقي له ما يبرره على الأقل من الناحية الأمنية.

من خلال ما سبق يتضح لنا التحديات التي تفرضها الشبكات الاجتماعية على أجهزة الأمن بصفة عامة. خاصة مع تزايد أنماط الاستخدامات الخطرة للشبكات الاجتماعية وتطبيقات الموبيل، في ظل صعوبة التعاون مع الشركات المشغلة لهذه الشبكات مثل "فيس بوك" و"تويتر" وغيرها، لملاحقة المطلوبين أمنياً، وهو ما يفرض على الدولة المصرية أن تتبنى سياسة وطنية تعيد فيها تعريف التهديدات الإلكترونية بصفة عامة، والتهديدات التي تطرحها الشبكات الاجتماعية بصفة خاصة، وأن تعيد النظر في التشريعات بما يعمل على وقف التهديدات الناجمة من الشبكات الاجتماعية، ويضمن الحفاظ على خصوصية الأفراد وحرية تبادل المعلومات في نفس الوقت، وأن تمتلك وتطور من الأدوات التكنولوجية ما يسمح لها بسرعة تعقب وكشف الجرائم، بهدف الحفاظ على أمن المواطنين وليس اختراق خصوصيتهم.

ويرجع ذلك إلى أن الشبكات الاجتماعية أصبحت واقعاً مؤثراً على كافة المفاهيم المتعلقة بالأمن القومي؛ سياسياً واقتصادياً وعسكرياً واجتماعياً. ومع تزايد عدد مستخدمي هذه الشبكات التي وصل إلى 2 مليار مستخدم، أصبح من الصعب منع التفاعلات التي تجري على هذه الشبكات. وكان للدور الذي لعبته هذه الشبكات في ثورات الربيع العربي أثر هام في تحول الأكاديميين والسياسيين نحوها؛ بهدف المشاركة في التفاعلات التي تجري عبرها أو تحليلها ودراستها. ومع تواجد الحركات الإرهابية والمنظمات الإجرامية عليها، تحولت أجهزة الأمن نحوها لمحاولة تفادي أخطارها.

وقد اتضح من خلال الدراسة، أن التوجه العام للدول بما فيها الدول الديمقراطية مثل الولايات المتحدة وبريطانيا، هو محاولة إحكام السيطرة على التفاعلات التي تجري على الشبكات الاجتماعية. إلا أن المشكلة في الحالة المصرية هي الجهة التي تقوم بالرقابة؛ فهناك عدم ثقة مجتمعية في أجهزة الأمن نتيجة موروث سلبي عبر عقود من الزمن في التعامل مع خصوصية المواطنين وحقوقهم في الحصول على المعلومات. ويبقى التخوف لدى المواطنين من إساءة أجهزة الأمن استخدام معلوماتهم الشخصية مشروعاً، حتى يقوم جهاز الأمن بتغيير الصورة الذهنية التي ترسخت في عقول المواطنين عبر سنوات طويلة عنه، وأن يقوم بناء جسور ثقة بينه وبين المجتمع، وأن يضمن الدستور والقانون حق المواطن في عدم انتهاك خصوصيته وإساءة استخدامها.

ومن ناحية أخرى يبقى أيضاً حق الدولة في الحفاظ على الأمن القومي مشروعاً، وكذلك عدم السماح لأي من الجماعات الإرهابية أو التخريبية أو الإجرامية باستخدام الشبكات الاجتماعية في العمليات اللوجستية وعمليات الحشد والتمويل لتنفيذ أعمال إجرامية. ويجب أن يتحقق ذلك من خلال تحديد مواطن الخطر والتهديد، ومراقبة الحسابات الإلكترونية التي تحرض على العنف وتدعو إلى الكراهية ونبذ الآخر وتكفيره، وأن تعمل أيضاً على الاستفادة من المميزات التي تقدمها الشبكات الاجتماعية سواء في قياس اتجاهات الرأي العام المتشكل عبرها، أو من خلال ما توفره من معلومات وشبكات علاقات قد تساعد في الكشف المبكر عن الجرائم قبل حدوثها. بالإضافة إلى ما توفره من عملية تواصل مباشر بين المسئولين والمواطنين وهو ما قد يساعد في كشف حالات الفساد وتمكين المواطنين من المشاركة المباشرة في إدارة حكم الدولة.

أما إشكالية العلاقة بين الخصوصية والأمن والحريات، فستظل متواجدة ولن تنتهي لأنها مثل بندول الساعة لا تتوقف في منطقة الوسط بل تمر عليها سريعاً، متوجهةً نحو اليمين الذي يمثل احترام خصوصية المواطنين وعدم انتهاكها مطلقاً، أو اليسار الذي يمثل المراقبة المشددة واقتحام الخصوصية وانتهاكها. والحل هو امتلاك الدولة إمكانيات الرقابة على الشبكات الاجتماعية، مع توفير الضمانات اللازمة للتأكد من عدم إساءة استعمال أجهزة الأمن للمعلومات الشخصية التي يتم تحصيلها جراء عملية المراقبة، ومحاسبتها في حالة إخلالها بذلك.

عن المؤلف إيهاب خليفة إيهاب عبد الحميد خليفة، رئيس وحدة متابعة التطورات التكنولوجية بمركز المستقبل للأبحاث والدراسات المتقدمة بأبو ظبي، وعضو هيئة التحرير بدورية "اتجاهات الأحداث" الصادرة عن مركز المستقبل. خريج كلية الاقتصاد والعلوم السياسية دفعة 2009 قسم العلوم السياسية، وحاصل على الماجيستير في العلوم السياسية حول "استخدامات القوة الإلكترونية في إدارة التفاعلات الدولية – دراسة حالة الولايات المتحدة الأمريكية من 2001 -2012". عمل باحثاً بمركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء خلال الفترة من 2009 -2014، وباحثاً متعاوناً بالمركز الإقليمي للدراسات الاستراتيجية بالقاهرة. شارك في عدد من المؤتمرات ونشر العديد من الأبحاث والأوراق العلمية حول الاستخدامات السياسية والعسكرية والاقتصادية للفضاء الإلكتروني.

يمكن التواصل من خلال ehabakhalifa@gmail.com

Notes

[←1]

الهوامش

Richard L. Kugler, “From Cyber Space To Cyber Power: Defining The Problems”, In Franklin D. Krammer, Stuart Starr, And Larry K. Wentz. Eds, Cyber Power And National Security, (Washington, D.C: National Defense Up, 2009), P316.

[←2]

د. سعاد محمود أبو ليلة، "دورة القوة: ديناميكيات الانتقال من "الصلبة" إلى " الناعمة" إلى "الافتراضية""، مجلة السياسة الدولية، ملحق اتجاهات نظرية:

القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية؟، العدد 188 (أبريل، 2012)، ص 16.

[←3]

Joseph Nye, Cyber Power, Joseph S. Nye, Cyber Power, (Harvard Kennedy School, May 2010), p3

[←4]

Daniel T. Kuehl, “From Cyber Space to Cyber Power: Defining the problems”, in Franklin D. Krammer, Stuart Starr, and Larry K. Wentz. Eds, cyber power and national security (Washington, D.C: National .defense up, 2009, p 48

[←5]

عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، (القاهرة، مركز الأهرام للدراسات السياسية والاستراتيجية، 2009)، ص ص 35-40

[←6]

.Joseph S. Nye, Cyber Power Op Cit. p4

[←7]

Daniel T. Kuehl, “From Cyber Space to Cyber Power: Defining the problems”, in Franklin D. Krammer, Stuart Starr, and Larry K. Wentz. Eds, cyber power and national security, (Washington, D.C: National .defense up, 2009(, p 16

[←8]

Franklin D. Kramer, Stuart H. Starr, Larry Wentz , eds, Cyberpower and National Security, (Washington D.C: National defense University, May .2009), p 48

[←9]

Joseph S. Nye, Cyber Power, Op. Cit, P3

[←10]
عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، (القاهرة، مركز الأهرام للدراسات السياسية والاستراتيجية، 2009)، ص ص 50- 58

[←11]

إيهاب عبد الحميد خليفة، القوة الإلكترونية والصراع الدولي، مقال منشور على موقع المركز العربي لأبحاث الفضاء الإلكتروني، بتاريخ 30 أغسطس 2013، يمكن المطالعة على:

http://www.accronline.com/print_article.aspx?id=15636 12

[←12]

عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، عدد رقم (188)، (أبريل 2012).

[←13]

"إدورد سنودن": متعاقد سابق مع وكالة الأمن القومي الأمريكي، واتهم بتسريب برامج سرية للحكومة الأمريكية عام 2013 خاصة بتجسس الولايات المتحدة على الاتصالات سواء الهاتفية أو عبر الانترنت، ومن أهما برنامج بريزم Prism.

[←14]

"جوليان أسانج": صحفي ومؤسس موقع ويكيليكس، والذي اتهم بتسريب ونشر ملايين الوثائق الخاصة بمراسلات الحكومة الأمركية مع سفاراتها في الخارج.

[<-15]

-سعود صالح كاتب، الإعلام الجديد وقضايا المجتمع: التحديات والفرص، 13- 15 ديسمبر2011، ورقة مقدمة للمؤتمر العالمي الثاني للإعلام الإسلامي، 2011.

[←16]

Danah m. boyd, Nicole B. Ellison, Social Network Sites: Definition, History, and Scholarship, .(Journal of Computer-Mediated Communication, 17 Dec 2007, vol(13), issue (1 http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/pdf

[←17]

lbackstrom, The Importance of Algorithms, topcoder, accessed on 10 may 2015 on https://www.topcoder.com/community/data-/science/data-science-tutorials/the-importance-of-algorithms

[←18]

Nicholas Diakopoulos, Sex, Violence, and Autocomplete Algorithms, .Slate, accessed 9 May 2015

http://www.slate.com/articles/technology/future_tense/2013/08/words_banned_from_bing and_google_s_autocomplete_algorithms.html_

[←19]

An Update to News Feed: What it Means for Businesses, facebook, :accessed on 11 may 2015, on

https://www.facebook.com/business/news/update-to-facebook-news-feed

[←20]

وليد رشاد زكي، الشبكات الاجتماعية. محاولة للفهم، مجلة السياسة الدولية، أبريل 2010، يمكن مطالعة المقال على الرابط التالي:

http://digital.ahram.org.eg/articles.aspx?Serial=148065&eid=897

[←21]

تعرف على تاريخ "الفيسبوك " بالصور، مجلة لغة العصر، 10-2-2015 يمكن المطالعة على الرابط التالي:

http://aitmag.ahram.org.eg/News/5354.aspx

[←22]
تاريخ الفيس بوك: جدول زمني عن التحديثات الرئيسية للفيس بوك، موقع تكنو دار، 12 أبريل 2015
/http://www.techno-dar.net/facebook-history-timeline-main-updates

[←23]

بعدما رفضت "فيس بوك" تعيينه.. مخترع "واتس آب" من عامل نظافة لملياردير، جريدة الوطن، 14 يوليو 2015، يمكن المطالعة على:

http://www.elwatannews.com/news/details/769799

[←24]

الفيس بوك تستحوذ على شبكات QuickFire، موقع عالم التقنية، 9 يناير 2015، يمكن المطالعة على:

http://www.tech-wd.com/wd/2015/01/09/%D8%A7%D9%84%D9%81%D9%8A%D8%B3-%D8%A8%D9%88%D9%83-%D8%AA%D8%B3%D8%AA%D8%AD%D9%88%D8%B0-%D8%B9%D9%84%D9%89-%D8%B4%D8%A8%D9%83%D8%A7%D8%AA-quickfire/

[←25]

فيس بوك تستحوذ على شركة متخصصة في تقنيات التعرف على الصوت، موقع عالم التقنية، 6 يناير 2015، للمطالعة http://www.tech-wd.com/wd/2015/01/06/%D9%81%D9%8A%D8%B3-%D8%A8%D9%88%D9%83-%D8%AA%D8%B3%D8%AA%D8%AD%D9%88%D8%B0-%D8%B9%D9%84%D9%89-%D8%B4%D8%B1%D9%83%D8%A9-%D9%85%D8%AA%D8%AE%D8%B5%D8%B5%D8%A9-%D9%81%D9%8A-%D8%AA%D9%82%D9%86%D9%8A%D8%A7/

[←26]

فيسبوك توفر الإنترنت مجانا على الهاتف المحمول بالهند، موقع العربية نت، 11 فبراير 2015، يمكن المطالعة على:

http://www.alarabiya.net/ar/technology/2015/02/11/%D9%81%D9%8A%D8%B3%D8%A8%D9%88%D9%83-%D8%AA%D9%88%D9%81%D8%B1-%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D9%85%D8%AC%D8%A7%D9%86%D9%8A-%D8%B9%D9%84%D9%89-%D8%A7%D9%84%D9%87%D8%A7%D8%AA%D9%81-%D8%A7%D9%84%D9%85%D8%AD%D9%85%D9%88%D9%84-%D9%81%D9%8A-%D8%A7%D9%84%D9%87%D9%86%D8%AF.html%

[←27]

10 شركات ضخمة حاولت شراء فيسبوك، موقع أرجيك، 14 أبريل 2014، للمطالعة:

http://www.arageek.com/2014/04/14/10-big-companies-wanted-to-buy-facebook.html

[←28]

المرجع السابق

[←29]

Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, the Guardia, 28 Jan 2014. On http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data

[←30]

البيانات الشخصية في قبضة ال CIA عبر "Angry bird"، موقع العربية نت، 28 يناير 2014، تاريخ مطالعة 15 فبراير 2015، يمكن المطالعة على:

http://www.alarabiya.net/ar/technology/2014/01/28/%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9-%D9%81%D9%8A-%D9%82%D8%A8%D8%B6%D8%A9-%D8%A7%D9%84%D9%80-CIA%D8%B9%D8%A8%D8%B1-Angry-bird-.html

[←31]

د. شادي عبد الوهاب، التفجير من الداخل: الملاح الأساسية لدوامة العنف في حروب الجيل الخامس، مجلة اتجاهات الأحداث، مركز المستقبل للدراسات والأبحاث المتقدمة، العدد الأول، أغسطس 2014 ص 12.

[←32]

Kenneth Geers, Cyber Space and the changing nature of warfare,(U.S. Representative Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia). On http://www.carlisle.army.mil/DIME/CyberSpace.cfm On August 15, 2013

[←33]

إيهاب خليفة، الكتائب الإلكترونية: حروب التواصل الاجتماعي في الشرق الأوسط، مجلة اتجاهات الأحداث، العدد4، (مركز المستقبل للأبحاث والدراسات المتقدمة، نوفمبر 2014)، ص ص 10 -16

[←34]

Justice Department and NSA memos proposing broader powers for NSA to collect data, the guardian, Access Date, August 26th, 2014, on http://www.theguardian.com/world/interactive/2013/jun/27/nsa-data-collection-justice-department

[←35]

Glenn Greenwald and Spencer Ackerman, How the NSA is still harvesting your online data, the guardian, August 26th, 2014 On: http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

[←36]

Pierluigi Paganini, Stellar Wind, Prism,EvilOlive,ShellTrumpet, US massive surveillance, security affairs, on June 29th, 2014, on http://securityaffairs.co/wordpress/15689/intelligence/stellar-wind-prism-evilolive-shelltrumpet-surveillance.html

[←37]

Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, Microsoft data , the verge, Access Date, August 25th, 2014, on http://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism/in/4167369

[←38] ,NSA Prism program slides, the guardian, On Nov 5th, 2013 http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

[←39]

Pentagon Seeks to Manipulate Social Media for Propaganda Purposes, global research, On http://www.globalresearch.ca/pentagon-seeks-to-manipulate-social-media-for-propaganda-purposes/25719 ,April 21th, 2014

[←40]

Nick Fielding and Ian Cobain, Revealed: US spy operation that manipulates social media, the guardian, On 21 March 2014, http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks

[←41]

Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, 28 January ,2014 http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data

[←42]

Sarah Lange, The End of: Social Media Revolution, fletche rforum, P59 http://www.fletcherforum.org/wp-content/uploads/2014/04/38-1_Lange1.pdf

[←43] تقرير قمة رواد التواصل الاجتماعي العرب، 2015 للمطالعة:
http://arabsmis.ae/reports/ASMISArabicReport.pdf

[←44]

«المصري اليوم» تنشر النص الكامل لملخص تقرير لجنة تقصي الحقائق حول ثورة 25 يناير، موقع المصري اليوم، تاريخ نشر 19 أبريل 2011، يمكن المطالعة على:

http://www.almasryalyoum.com/news/details/126472

[←45]

تأكيدا لانفراد "الوطن".. "الداخلية" تبدأ تنفيذ "القبضة الإلكترونية" على مواقع التواصل الاجتماعي، جريدة الوطن، 18 سبتمبر 2014، يمكن المطالعة على:

http://www.elwatannews.com/news/details/561213

[←46]

المادة 57 من الدستور المصري المعدل عام 2013، الباب الثالث الحقوق والحريات والواجبات العامة، ص 19.

[←47]

مصدر أمني: الداخلية أوقفت مشروع مراقبة فيسبوك وتويتر لحين البت بالدعوى، جريدة الشروق، 31 أكتوبر 2014.

http://www.shorouknews.com/news/view.aspx?cdate=31102014&id=6598ad63-c912-4cd4-86fe-485abe3524db

[←48]

تأكيدا لانفراد "الوطن".. "الداخلية" تبدأ تنفيذ "القبضة الإلكترونية" على مواقع التواصل الاجتماعي، موقع الوطن، 18 سبتمبر 2014.

http://www.elwatannews.com/news/details/561213

[←49]

إيهاب خليفة، الأبعاد المختلفة لإدارة الرقابة على الشبكات الاجتماعية في مصر، سلسلة بدائل، عدد 11، (مركز الأهرام للدراسات السياسية والاستراتيجية، أبريل 2015).

[←50]

أنظر: موقع جريدة الفجر عدد 15 أكتوبر 2011.

[←51]

سحر عزام وعبير القاضر، "أبرز شائعات عام 2014 "، موقع مصراوى، 26 ديسمبر 2014:

http://www.masrawy.com/News/yearender14-political/details/2014/12/26/416981/أبرز-شائعات-2014

[←52]

إيهاب خليفة،" الجيل الرابع: تحولات قادمة فى استخدامات الشبكات الاجتماعية"، مرجع سبق ذكره.

[←53]

United Nations, International Narcotics Board, incb, 2012, March :2013

http://www.incb.org/documents/Publications/AnnualReports/AR2012/AR_2012_E.pdf

[←54]

Andrew Osborn (editor), "Social media used to sell drugs to youth, :report says", Reuters, Feb 28, 2012

http://www.reuters.com/assets/print?aid=USTRE81R1A320120228

[←55]

Raf Sanchez, US wages social media war against Isil, Telegraph, 25 Sep 2014, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11122490/US-wages-social-media-war-against-Isil.html

[←56]

Geoff Dean, Peter Bell, Jack Newan, "The Dark Side of Social Media: Review of Online Terrorism", Pakistan Journal of Criminology, Vol. 3, .No. 4, April – July 2012, PP. 194 -195

[←57]

سماح عبد الصبور، "الإرهاب الرقمي: أنماط استخدام الجماعات المسلحة للإرهاب الشبكي"، موقع مركز المستقبل للأبحاث والدراسات المتقدمة، 2 أكتوبر 2014:

http://www.futurecenter.ae/analys.php?analys=251

[←58]

محمد فوزى وشيماء بدوى، " بزنس الأسلحة «الآلية» و«البيضاء» ينشط على فيس بوك"، موقع البورصة نيوز، أكتوبر 2014:

http://www.alborsanews.com/2014/10/22/%D8%A8%D8%B2%D9%86%D8%B3-%D8%A7%D9%84%D8%A3%D8%B3%D9%84%D8%AD%D8%A9-%D8%A7%D9%84%D8%A2%D9%84%D9%8A%D8%A9-%D9%88%D8%A7%D9%84%D8%A8%D9%8A%D8%B6%D8%A7%D8%A1-%D9%8A%D9%86%D8%B4/

[←59]
سماح عبد الصبور، "الإرهاب الرقمي: أنماط استخدام الجماعات المسلحة للإرهاب الشبكي"، موقع مركز المستقبل للأبحاث والدراسات المتقدمة، 2 أكتوبر 2014: http://www.futurecenter.ae/analys.php?analys=251

[←60]

نجاة عطية الجبالي وإمام رمضان، "تعرف على طريقة غلق "مواقع التكفير" وبدائل قادة الإرهاب لإجهاض دعوة "السيسي""، موقع صدى البلد، 11 يناير 2015:

http://www.el-balad.com/1334422

[←61]

الأناضول، "بيعة إليكترونية لأميرة دولة الخلافة أبو بكر البغدادي"، موقع المصري اليوم، 2 يوليو 2014:

http://www.almasryalyoum.com/news/details/475090

[←62]

إيهاب خليفة، الأبعاد المختلفة لإدارة الرقابة على الشبكات الاجتماعية في مصر، مرجع سبق ذكره.

[←63]

هو تطوير لقانون مراقبة الاستخبارات الخارجية Foreign Intelligence Surveillance Act، بهدف تمكين الولايات المتحدة من مراقبة أنشطة الجماعات الإرهابية بعد أحداث 11 سبتمبر، نص القانون متاح على الرابط التالي:http://www.justice.gov/archive/ll/

[←64]

:NSA Prism program slides", The Guardian, On Nov 5th, 2013"

http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

[←65]

Dan Seifert, “Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, :Microsoft data” ,The Verge, June 6th, 2013 http://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism

[←66]

Timothy B. Lee, "Here's everything we know about PRISM to date", Washington Post, June 12, 2013 http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-/we-know-about-prism-to-date

[←67]

.Ibid

[←68]

US Department of homeland security , Privacy Compliance Review of the NOC Publicly Available Social Media Monitoring and Situational :Awareness Initiative Privacy Compliance Review, 2012, Nov 8, 2012

http://www.dhs.gov/sites/default/files/publications/privacy/PCRs/PCR%20NOC%20Situational%20Awareness%20Initiative%20%28FINAL%29%2020121108.pdf

[←69]

“وزارة الامن الداخلي الامريكية تتابع تويتر وفيسبوك”، موقع رويترز، 12 يناير 2012:

http://ara.reuters.com/article/internetNews/idARACAE80B07B20120112

[←70] الحكومة الأمريكية تستغل تطبيقات الهواتف لأغراض التجسس، aitnews، يناير 2014 http://aitnews.com/2014/01/28/%D8%AA%D9%82%D8%B1%D9%8A%D8%B1-%D8%A7%D9%84%D8%AD%D9%83%D9%88%D9%85%D8%A9-%D8%A7%D9%84%D8%A3%D9%85%D8%B1%D9%8A%D9%83%D9%8A%D8%A9-%D8%AA%D8%B3%D8%AA%D8%BA%D9%84-%D8%AA%D8%B7%D8%A8%D9%8A%D9%82%D8%A7/

[←71]

Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for “ :user data”, The Guardian, Jan 28th,2014

http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data

[←72]

إيهاب خليفة، "الجيل الرابع: تحولات قادمة في استخدامات الشبكات الاجتماعية"، مرجع سبق ذكره.

[←73]

"البيانات الشخصية في قبضة ال CIA عبر،”"Angry bird"، موقع العربية، 28 يناير 2014:

http://www.alarabiya.net/ar/technology/2014/01/28/%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9-%D9%81%D9%8A-%D9%82%D8%A8%D8%B6%D8%A9-%D8%A7%D9%84%D9%80-%CIA%D8%B9%D8%A8%D8%B1-Angry-bird-.html

[←74]

"الحكومة الأمريكية تستغل تطبيقات الهواتف لأغراض التجسس"، مرجع سبق ذكره.

[←75]

Social media mass surveillance is permitted by law, says top UK“ :official”, The Guardian, 17 June, 2014

http://www.theguardian.com/world/2014/jun/17/mass-surveillance-social-media-permitted-uk-law-charles-farr

[←76]

عبد الاله مجبد، "بريطانيا تصنف مواقع التواصل الاجتماعي ضمن مثيري الشغب"، موقع إيلاف، 12 أغسطس 2011:

http://www.elaph.com/Web/technology/2011/8/675500.html

[←77]

Paul Wright, “Meet Prism's little brother: Socmint”, Wired.com, 26 :june 2013

http://www.wired.co.uk/news/archive/2013-06/26/socmint

[←78]

"مشروع قانون بريطاني يسمح بتسليم بيانات مستخدمي الإنترنت للأجهزة الأمنية"، موقع البي بي سي، نوفمبر 2014:

http://www.bbc.co.uk/arabic/scienceandtech/2014/11/141123_internet_bill_uk

[←79]

مروان شلالا، "الكتيبة 77: وحدة الحرب الالكترونية في الجيش البريطاني"، موقع إيلاف، 31 يناير 2015:

http://www.elaph.com/Web/News/2015/1/979088.html

[←80]

أشهر 15 دولة مارست الحجب الكلي أو المؤقت لمواقع التواصل الاجتماعي، موقع ساسة بوست، 4 يونيو 2014، يمكن المطالعة على
http://www.sasapost.com/countries-blocked-social-networks/

[←81]

Twitter Grows Stronger in Mexico, Emarketer Report 2012, on http://www.emarketer.com/Article.aspx?R=1009370&ecid=a6506033675d47f881651943c21c5ed4

[←82]

لجنة مكلفة مراقبة الإنترنت تهدد الحكومة الايرانية باغلاق موقع انستغرام، موقع إيلاف، 11 نوفمبر 2014، يمكن المطالعة على:

http://www.elaph.com/Web/News/2014/11/957323.html#sthash.0o4ItZDv.dpuf

[←83]

هل ترفع إيران الحظر عن مواقع التواصل الاجتماعي؟، موقع راديو سوا، 7 يناير 2013، يمكن المطالعة على:

http://www.radiosawa.com/content/will-iran-lift-ban-social-media-websites/217441.html#ixzz3L3b0qW5c

[←84]

إيهاب خليفة، الأبعاد المختلفة لإدارة الرقابة على الشبكات الاجتماعية في مصر، مرجع سبق ذكره.

[←85]

.Sarah Lange, Op.Cit, PP. 47-68

[←86]

الهند تطالب «بلاك بيري» و«سكايبي» و«جوجل» بإنشاء خوادم محلية، جريدة الاتحاد، 2 سبتمبر 2010، للمطالعة:

http://manager.alittihad.ae/details.php?id=55803&y=2010

[←87]

الإمارات تفك شفرة "بلاك بيري"، شبكة مصرس، 18 ديسمبر 2010، للمطالعة على:

http://www.masress.com/alwafd/5968

[←88]

تأسس المركز المصري في أبريل عام 2009 من قبل الجهاز القومي لتنظيم الاتصالات التابع لوزارة الاتصالات، حيث يعمل به فريق من 16 متخصصاً، وذلك لتقديم الدعم الفني على مدار 24 ساعة لحماية البنية التحتية الحيوية للمعلومات.